

User's Guide

**TRENDnet<sup>®</sup>**



**N150 Wireless ADSL 2+ Modem Router**

**TEW-721BRM**

## Contents

<b>Product Overview .....</b>	<b>1</b>
Package Contents .....	1
Features .....	1
Product Hardware Features.....	2
Application Diagram .....	4
<b>Basic Router Setup .....</b>	<b>5</b>
Creating a Home Network .....	5
Router Installation .....	6
Connect additional wired devices to your network.....	10
<b>Wireless Networking and Security .....</b>	<b>10</b>
How to choose the type of security for your wireless network .....	10
Secure your wireless network .....	11
Connect wireless devices to your router .....	13
Connect wireless devices using WPS .....	13
Basic wireless settings .....	14
Guest Network.....	15
Steps to improve wireless connectivity .....	16
Advanced wireless settings.....	17
Multiple SSID .....	17
Additional Wireless Settings .....	17
<b>Access Control Filters .....</b>	<b>18</b>
Access control basics .....	18
Wireless MAC address filters .....	18
MAC address filters .....	19
URL/Keyword Blocking .....	19

Domain Filters .....	19
IP Filtering .....	20
Packet Filters .....	20
<b>Advanced Router Setup .....</b>	<b>22</b>
Access your router management page.....	22
Change your router login password .....	23
Set your router date and time .....	23
Manually configure your Internet connection .....	24
Change your router IP address .....	28
Set up the DHCP server on your router .....	29
Enable/disable UPnP on your router .....	30
Allow/deny VPN connections through your router .....	30
Configure ALG settings .....	31
Additional Security Settings.....	31
Allow/deny multicast streaming.....	32
Identify your network on the Internet .....	33
Allow remote access to your router management page .....	34
Configure remote access rules .....	34
Configure the router's Ethernet port settings .....	35
Open a device on your network to the Internet.....	35
DMZ.....	35
Virtual Server .....	36
Port Trigger .....	37
Prioritize traffic using QoS (Quality of Service) .....	38
Create schedules .....	39
Add static routes to your router.....	39
Enable dynamic routing on your router .....	40

Setup Port Mapping.....	41	Check the router DSL Statistics.....	50
Setup IPv6 on your router .....	41	View your router log .....	51
Configure ADSL settings.....	42	View your router traffic .....	51
<b>Router Maintenance &amp; Monitoring.....</b>	<b>42</b>	Configure your router log .....	52
Reset your router to factory defaults .....	42	Enable SNMP on your router .....	53
Router Default Settings .....	43	Enable TR-069 on your router .....	54
Backup and restore your router configuration settings .....	44	<b>Troubleshooting .....</b>	<b>55</b>
Restart your router .....	46	<b>Appendix .....</b>	<b>56</b>
Check connectivity using the router management page .....	46		
Manage Initialization Scripts .....	46		
Check Internet connectivity using the router management page .....	47		
Check the router system information.....	47		
Check the router IPv6 status.....	49		
Check the router IPv6 status.....	49		
Check the router Wireless clients .....	49		
Check the router LAN clients .....	50		
Check the router Routing Table .....	50		
Check the router Basic Statistics.....	50		

## Product Overview



**TEW-721BRM**

## Package Contents

In addition to your router, the package includes:

- Multi-Language Quick Installation Guide
- CD-ROM (User's Guide)
- Network cable (1.5m / 5ft.)
- RJ-11 telephone cable (1.8m / 5ft.)
- Power adapter (12V DC, 0.5A)

If any package contents are missing or damaged, please contact the retail store, online retailer, or reseller/distributor from which the product was purchased.

## Features

TRENDnet's N150 Wireless ADSL 2+ Modem Router, model TEW-721BRM, is a combination high performance modem for Internet access and reliable wireless N150 router—well suited for small to medium size homes. The modem is compatible with most ADSL Internet service provider networks and it comes with an intuitive guided setup wizard. For your convenience the wireless network is setup and pre-encrypted out of the box.

## Features

### Easy Setup

Get up and running in minutes with the intuitive guided setup

### Internet Service

Compatible with most ADSL 2/2+ internet service provider networks

### IPv6

IPv6 network support

### N150 Wireless

Reliable 150 Mbps Wireless N

### Pre-Encrypted Wireless

For your convenience the wireless network arrives pre-encrypted with its own unique password

### Guest Network

Create an isolated network for guest internet access only

### Wireless On/Off Button

Enable or disable the wireless network with the convenient on/off wireless button

### One Touch Connection

Connect to the router at the touch of the Wi-Fi Protected Setup (WPS) button

### Parental Controls

Control access to specific websites and manage which devices can access the router

### Advanced QoS

Classify and prioritize different types of data such as video and audio transmissions

### Energy Savings

Embedded GREENnet technology reduces power consumption by up to 50%

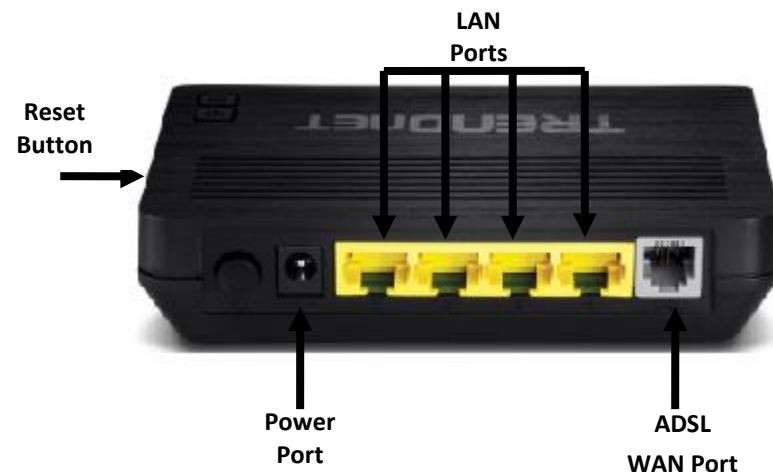
### Ethernet Ports

Four Ethernet ports to hardwire devices

\*Maximum wireless signal rates are referenced from IEEE 802.11 theoretical specifications. Actual data throughput and coverage will vary depending on interference, network traffic, building materials and other conditions.

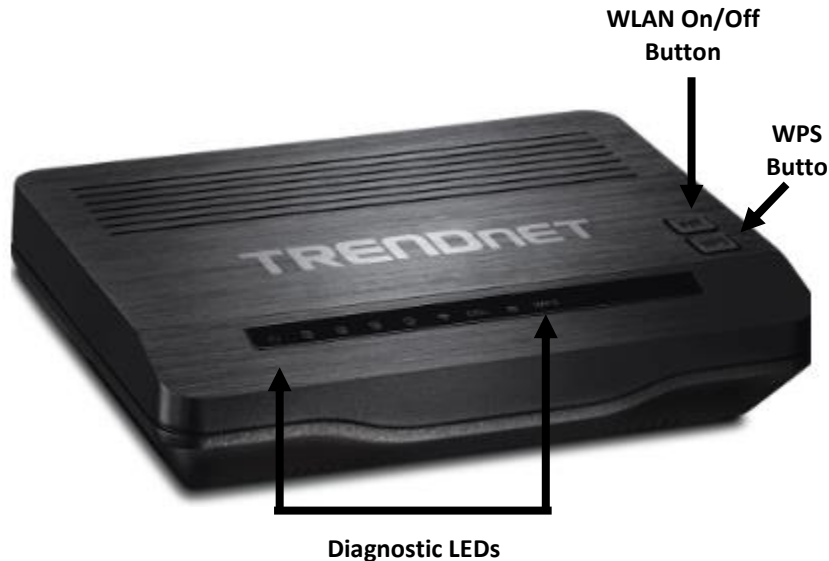
## Product Hardware Features

### Rear View



- **On/Off Power Button:** Push to power on or off router.
- **Power Port:** Connect the included power adapter from your modem router power port and to an available power outlet.  
**Note:** Use only the adapter that came with your router.
- **LAN Ports:** Connect Network cables (also called network cables) from your modem router LAN ports to your wired network devices.
- **ADSL WAN Port (RJ-11 telephone port):** Connect an RJ-11 telephone cable from your modem router ADSL WAN port to your telephone jack/DSL line.
- **Reset Button:** Push and hold this button for **10** seconds and release to reset your router to its factory defaults.

## Front View



- **WLAN On/Off:** Press button to turn off or on wireless network.
- **WPS Button:** Push button to activate WPS (WiFi Protected Setup) push and hold this button for **3** seconds and release to activate WPS. Within 2 minutes, push and hold the WPS button on your wireless client device. WLAN LED indicator will blink rapidly to indicate that WPS has been activated.
- **Diagnostic LEDs:**
  - **Power LED:** This LED indicator is blinks green when properly connected to a power supply. When the device is malfunctioned LED indicator will be red.

- **LAN 1-4 (Link/Activity) LEDs** – These LED indicators are solid green when the LAN ports are successfully connected to your wired network devices (which are turned on). These LED indicators will blink green while data is transmitted or received through your modem router's LAN ports.
- **Wireless WLAN (Link/Activity) LED:** This LED indicator is solid green when the wireless is "On" and functioning properly on your modem router. This LED indicator will be blinking while data is transmitted or received by your wireless clients or wireless network devices connected to your modem router. This LED indicator will be off when the wireless functionality of your modem router is disabled.
- **ADSL WAN (Link/Activity) LED:** This LED indicator is blinking green when the ADSL status of the modem router is ready to establish connection to your ISP. The LED indicator will turn solid green when the modem router has been properly configured with the settings provided by your ISP and successful ADSL connection has been made to your ISP. This LED indicator will be blink while data is transmitted or received through the ADSL port of your modem router.
- **Internet:** This LED Indicator is solid green with valid internet connection. The LED indicator blinks green during data transmission. If the indicator is red, this indicates invalid internet connection.
- **WPS LED:** This LED indicator blinks green when WPS is activated. The LED will stop blinking and remain solid when WPS is completed. When the indicator blinks red it indicates there was no WPS device connected.

## Application Diagram



The router is installed near the wall telephone jack/DSL line (DSL service supplied by your ISP "Internet Service Provider") which connects to the Internet. Wireless signals from the router are broadcasted to wireless clients such as laptops (with wireless capability) thereby providing Internet access.

## Basic Router Setup

### Creating a Home Network

What is a network?

A network is a group of computers or devices that can communicate with each other. A home network of more than one computer or device also typically includes Internet access, which requires a router.

A typical home network may include multiple computers, a media player/server, a printer, a modem, and a router. A large home network may also have a switch, additional routers, access points, and many Internet-capable media devices such as TVs, game consoles, and Internet cameras.

- **Modem:** Connects a computer or router to the Internet or ISP (Internet Service Provider).  
***Note:** The TEW-721BRM is a combination DSL modem and router, therefore, you do not require a separate DSL modem from your ISP when setting up this product.*
- **Router:** Connects multiple devices to the Internet.
- **Switch:** Connect several wired network devices to your home network. Your router has a built-in network switch (the LAN port 1-4). If you have more wired network devices than available Network ports on your router, you will need an additional switch to add more wired connections.

### How to set up a home network

1. For a network that includes Internet access, you'll need:
  - Computers/devices with a Network port or wireless networking capabilities.
  - A modem and Internet service to your home, provided by your ISP (modem typically supplied by your ISP).
  - A router to connect multiple devices to the Internet.
2. Set up your router. See "How to setup your router" below.
3. To connect additional wired computers or wired network devices to your network, see "Connect additional wired devices to your network" on page 11.
4. To set up wireless networking on your router, see "Wireless Networking and Security" on [page 11](#).

### How to setup your router

Refer to the Quick Installation Guide or continue to the next section "Router Installation" on page 6 for more detailed installation instructions.

### Where to find more help

In addition to this User's Guide, you can find help below:

- <http://www.trendnet.com/support>  
(documents, downloads, and FAQs are available from this Web page))



## Router Installation

### Before you Install

Many Internet Service Providers (ISPs) allow your router to connect to the Internet without verifying the information fields listed below. Skip this section for now and if your router cannot connect to the Internet using the standard installation process, come back to this page and contact your ISP to verify required ISP specification fields listed below.

### General ADSL Parameters

VCI: \_\_\_\_\_

VPI: \_\_\_\_\_

MTU: \_\_\_\_\_

Data Encapsulation (LLC/VCMux) : \_\_\_\_\_

Schedule Type (UBR/CBR/VBR/GFR): \_\_\_\_\_

VLAN Tag (If required by your ISP): \_\_\_\_\_

### ADSL Connection Types:

#### 1. Ethernet over ATM (RFC 1483 Bridged) with NAT

- **1a. Obtain IP Address Automatically (Dynamic IP Address)**

Host Name (Optional) \_\_\_\_\_

ISP registered Mac Address or Clone MAC address (Optional)\_\_\_\_:\_\_\_\_:\_\_\_\_:\_\_\_\_:\_\_\_\_:\_\_\_\_

- **1b. Fixed IP address (Static IP Address)**

WAN IP Address: \_\_\_\_\_ (e.g. 215.24.24.129)

WAN Subnet Mask: \_\_\_\_\_

WAN Gateway IP Address: \_\_\_\_\_

Primary DNS Server Address: \_\_\_\_\_

Secondary DNS Server Address: \_\_\_\_\_

#### 2. IP over ATM (RFC 1483 Routed)

- **2a. Obtain IP Address Automatically (Dynamic IP Address)**

Host Name (Optional) \_\_\_\_\_

ISP registered Mac Address or Clone MAC address (Optional)\_\_\_\_:\_\_\_\_:\_\_\_\_:\_\_\_\_:\_\_\_\_:\_\_\_\_

- **2b . Fixed IP address (Static IP Address)**

WAN IP Address: \_\_\_\_\_ (e.g. 215.24.24.129)

WAN Subnet Mask: \_\_\_\_\_

WAN Gateway IP Address: \_\_\_\_\_

Primary DNS Server Address: \_\_\_\_\_

Secondary DNS Server Address: \_\_\_\_\_

### 3. PPP over ATM (PPPoE)

- **3a. PPPoE to obtain IP automatically**

Account/User Name: \_\_\_\_\_

Password: \_\_\_\_\_

- **3b. PPPoE with a fixed IP address**

User Name: \_\_\_\_\_

Password: \_\_\_\_\_

Verify Password: \_\_\_\_\_

IP Address: \_\_\_\_\_ (e.g. 215.24.24.129)

Primary DNS Server Address: \_\_\_\_\_

Secondary DNS Server Address: \_\_\_\_\_

### 4. PPP over Ethernet (PPPoA)

- **4a. PPPoA to obtain IP automatically**

Account/User Name: \_\_\_\_\_

Password: \_\_\_\_\_

- **4b. PPPoA with a fixed IP address**

User Name: \_\_\_\_\_

Password: \_\_\_\_\_

Verify Password: \_\_\_\_\_

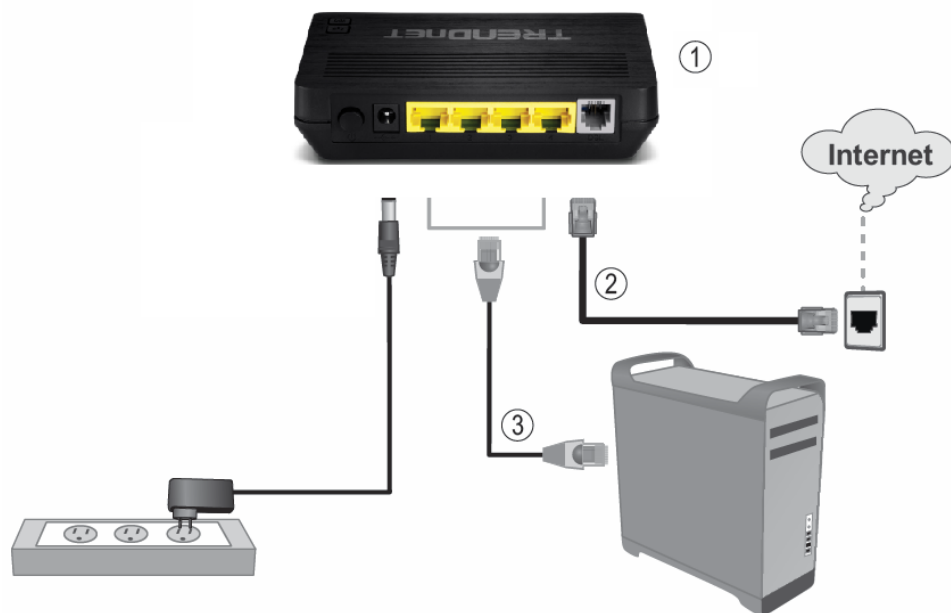
IP Address: \_\_\_\_\_ (e.g. 215.24.24.129)

Primary DNS Server Address: \_\_\_\_\_

Secondary DNS Server Address: \_\_\_\_\_

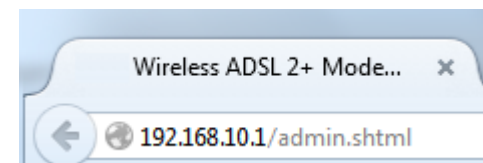
## Hardware Installation

1. Connect the detachable antenna to your modem router.
2. Connect one end of the RJ-11 telephone cable to the modem router ADSL port.  
Connect the other end of the RJ-11 telephone cable to the telephone jack/DSL line.
3. Using the Network cable, connect your computer to one of the four LAN ports on the modem router.
4. Connect the power adapter to the modem router and then to a power outlet.
5. Verify that the status LED indicators on the front of the modem to confirm the device is fully functional: Status (Green), ADSL (Green), WLAN (Green) and the LAN port (1,2,3,4) (Green) your computer is connected.

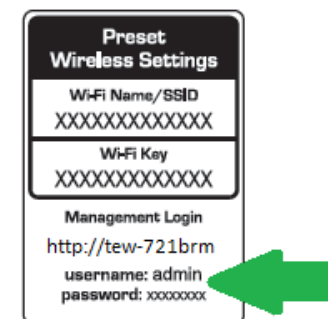


## Setup Wizard

1. Open your web browser (e.g. Internet Explorer, Firefox, Safari, Chrome, or Opera) and go to <http://192.168.10.1>. Your router will prompt you for a user name and password.



2. Your router will prompt you for a user name and password. For added security, the router is preconfigured with a unique password. You can find the **Password** on a sticker on the side of the router and on the label on the bottom of the router.



3. Enter your **Username** and **Password**, select your preferred language, and then click **Login**.

Login to the TEW-721BRM	
User Name:	<input type="text"/>
Password:	<input type="password"/>
Language:	English <span>▼</span>
<input type="button" value="Login"/>	

3. The Setup Wizard will automatically appear. This section determines what method the router will use to interface with your ISP service. Select the ADSL Internet connection type provided by your ISP and click Next.

**Note:** If the Setup Wizard does not automatically appear, click Setup Wizard (the top button on the left tab).

Internet Settings
<input checked="" type="radio"/> PPPoE (RFC-2516 PPP over Ethernet)
<input type="radio"/> PPPoA (RFC-2364 PPP over ATM)
<input type="radio"/> IPoA (RFC-1483 Routed)
<input type="radio"/> Dynamic IP Address (IPoEoA/MER(MAC Encapsulated Routed) with DHCP)
<input type="radio"/> Static IP Address
<input type="radio"/> Bridge Mode (RFC-1483 Bridged)
<input type="radio"/> CIP (RFC-1577 Classic IP/ARP over ATM)

**Note:** It is strongly recommended to contact your ISP to verify all required settings for one of the options listed on page 6. The options listed on page 6 match the settings options available to choose from

4. The Setup Wizard can automatically detect your VPI/VCI and Data Encapsulation settings of your ADSL connection. Select Auto-detect and click Next.

Determine Connection Method Select
<input checked="" type="radio"/> Auto-detect
<input type="radio"/> Manual Selection

**Note:** If you encounter any issues with the Auto-Detect feature on the wizard, you can click "Skip Scan", and configure your ADSL connection settings manually.

5. Once the wizard detects your VPI/VCI settings you can verify if the values are correct and click Next to continue.

Internet Connection Settings	
Profile Name	pvc0_8_35
Enable AutoPVC	Disable
VPI	0 (0~255)
VCI	35 (32~65535)
Encapsulation	LLC
ATMQoS	UBR
Peak Cell Rate	6000 (0~6000 cells/s)
Backup VLAN ID	0 (0~4095)
Enable Default Vlan	Disable
PPPoE PassThrough	Disable

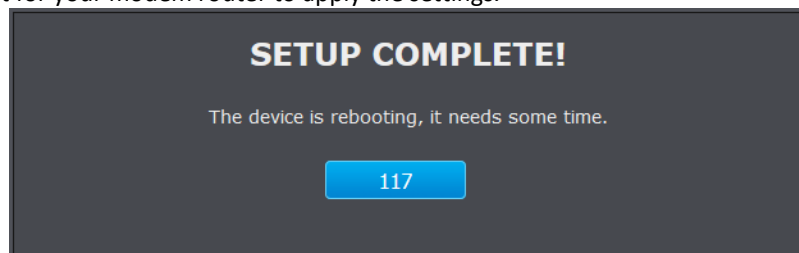
6. The following screen will appear next, depending the ADSL connection type you selected, you may need to enter additional information such as your PPPoE/PPPoA user name and password information provided by your ISP static IP. Enter any additional information required by your ISP for your ADSL connection and click Next.

PPPoE (RFC-2516 PPP over Ethernet)	
IP Protocol Version	<input checked="" type="radio"/> IPv4 only <input type="radio"/> IPv4/v6 both <input type="radio"/> IPv6 only
IP Mode of Connection	Dynamic
Name	pppoe
NAT	Enable
User Name	500493@bzn
User Password	*****
Confirm Password	*****
Max MRU	1492 (576~1492)
DNS Enabled	Enable
DNS Override Allowed	Disable
DNS Server 1	(optional)
DNS Server 2	(optional)
PPPoE Service Name	(optional)
MAC Address	00 : 18 : E7 : 5C : 42 : E9 <a href="#">Clone MAC</a>
PPPoE AC Name	(optional)
Connection Trigger	AlwaysOn
Idle Disconnect Time	300 (30~3600 seconds)
LCP Interval	20 (0~86400 seconds)
As system default route	<input checked="" type="checkbox"/> (Current setting: pppoe)
ICMP Reply Enable	<input checked="" type="checkbox"/>
Proxy ARP Enable	<input type="checkbox"/>

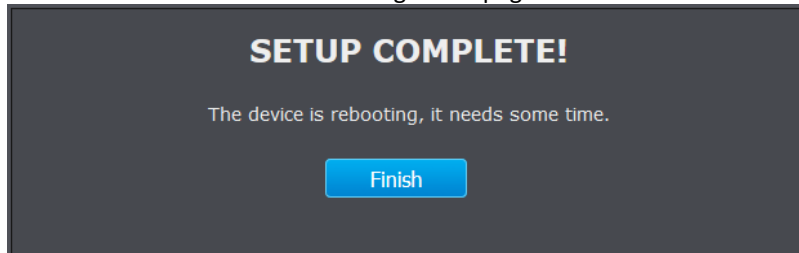
7. The Summary page will allow you to quickly review the settings you applied in the Setup Wizard. Click Save to apply settings.

Information	
WAN IP Address:	68.167.159.22
WAN DNS Server:	64.105.132.251,64.105.172.27
WAN MAC Address:	00:18:E7:5C:42:E9
IP Address	192.168.10.1
MAC Address	00:18:E7:5C:42:E9
SSID	72
Authentication Type	WPA2-AES-PSK

8. Wait for your modem router to apply the settings.

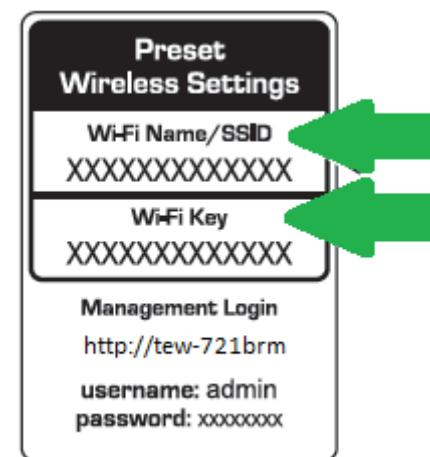


9. Click Finish to return to the router management page.



**Note:** If you cannot access the Internet, please verify your hardware connections and LED status and re-run the Setup Wizard to verify you have applied the correct settings.

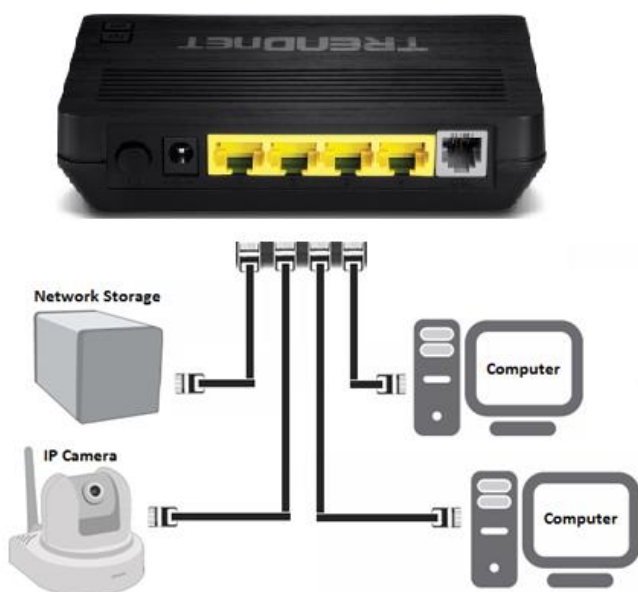
10. For added security, the router is pre-encrypted with its own unique wireless network security key. You can find the unique network security key and pre-assigned network name (SSID) on a sticker on the front of the router and on a label on the bottom of the router. If you would like to change the wireless settings, continue to the next page to launch the wireless setup wizard.



## Connect additional wired devices to your network

You can connect additional computers or other network enabled devices to your network by using Network cables. Connect them to one of the available LAN ports labeled 1,2,3,4 on your modem router. Check the status of the LED indicators (1, 2, 3, or 4) on the front panel of your router to ensure the physical cable connection from your computer or device.

**Note:** If you encounter issues connecting to your network, there may be a problem with your computer or device network settings. Please ensure that your computer or device network settings (also called TCP/IP settings) are configured to obtain IP address settings automatically (also called dynamic IP address or DHCP) and to Obtain DNS Server address settings automatically.



## Wireless Networking and Security

### How to choose the type of security for your wireless network

Setting up wireless security is very important. Leaving your wireless network open and unsecure could expose your entire network and personal files to outsiders. TRENDnet recommends reading through this entire section and setting up wireless security on your new router.

There are a few different wireless security types supported in wireless networking each having its own characteristics which may be more suitable for your wireless network taking into consideration compatibility, performance, as well as the security strength along with using older wireless networking hardware (also called legacy hardware).

It is strongly recommended to enable wireless security to prevent unwanted users from accessing your network and network resources (personal documents, media, etc.).

In general, it is recommended that you choose the security type with the highest strength and performance supported by the wireless computers and devices in your network. Please review the security types to determine which one you should use for your network.

#### Wireless Encryption Types

- **WEP:** Legacy encryption method supported by older 802.11b/g hardware. This is the oldest and least secure type of wireless encryption. It is generally not recommended to use this encryption standard, however if you have old 802.11 b or 802.11g wireless adapters or computers with old embedded wireless cards(wireless clients), you may have to set your router to WEP to allow the old adapters to connect to the router. **Note:** This encryption standard will limit connection speeds to 54Mbps.
- **WPA:** This encryption is significantly more robust than the WEP technology. Much of the older 802.11g hardware was been upgraded (with firmware/driver upgrades) to support this encryption standard. Total wireless speeds under this encryption type however are limited to 54Mbps.
- **WPA / WPA2:** This setting provides the router with the ability to detect wireless devices using either WPA or WPA2 encryption. Your wireless network will automatically change the encryption setting based on the first wireless device connected. For example, if the first wireless client that connects to your wireless

network uses WPA encryption your wireless network will use WPA encryption. Only when all wireless clients disconnect to the network and a wireless client with WPA2 encryption connects your wireless network will then change to WPA2 encryption. NOTE: WPA2 encryption supports 802.11n speeds and WPA encryption will limit your connection speeds to 54Mbps

- **WPA2:** This is the most secure wireless encryption available today, similar to WPA encryption but more robust. This encryption standard also supports the highest connection speeds. TRENDnet recommends setting your router to this encryption standard. If you find that one of your wireless network devices does not support WPA2 encryption, then set your router to either WPA or WPA-Auto encryption.

**Note:** Check the specifications of your wireless network adapters and wireless appliances to verify the highest level of encryption supported. Below is brief comparison chart of the wireless security types and the recommended configuration depending on which type you choose for your wireless network.

Security Standard	WEP	WPA	WPA2
<b>Compatible Wireless Standards</b>	IEEE 802.11a/b/g/n (802.11n devices will operate at 802.11g speeds)	IEEE 802.11a/b/g/n (802.11n devices will operate at 802.11g speeds)	IEEE 802.11a/b/g/n
<b>Highest Performance Under This Setting</b>	Up to 54Mbps	Up to 54Mbps	Up to 450Mbps*
<b>Encryption Strength</b>	Low	Medium	High
<b>Additional Options</b>	Open System or Shared Key, HEX or ASCII, Different key sizes	TKIP or AES, Preshared Key or RADIUS	TKIP or AES, Preshared Key or RADIUS
<b>Recommended Configuration</b>	Open System ASCII 13 characters	TKIP Preshared Key 8-63 characters	AES Preshared Key 8-63 characters

\*Dependent on the maximum 802.11n data rate supported by the device (150Mbps, 300Mbps, or 450Mbps)

## Secure your wireless network

Setup > Wireless Settings

After you have determined which security type to use for your wireless network (see “How to choose the security type for your wireless network” on page 12), you can set up wireless security.

1. Log into your router management page (see “Access your router management page” on [page 22](#)).
2. Click on **Setup**, and click on **Wireless Settings**.
3. Click on the **Security Mode** drop-down list to select your wireless security type.

### Selecting WEP:

If selecting **WEP** (Wired Equivalent Privacy), please review the WEP settings to configure and click **Apply** to save the changes.

- **Authentication Type:** Choose **Open**, **Shared**, or **Auto**.

**Note:** It is recommended to use Open System because it is known to be more secure than Shared Key.

- **WEP Key 1-4**

- Choose **HEX** or **ASCII**.

**Note:** It is recommended to use ASCII because of the much larger character set that can be used to create the key.

- This is where you enter the password or key needed for a computer to connect to the router wirelessly
- You can define up to 4 passwords or 4 keys. Only one key can be active at a given time. Most users simply define one key.
- Choose a key index 1, 2, 3, or 4 and enter the key.
- When connecting to the router, the client must match both the password and the Key number. (e.g. if you have activated Key 2 with a password of 12345, then the client must select: Key 2 (entering Key 1, 3, or 4 will block the ability to connect) and enter password 12345)

**Selecting WPA-PSK, WPA-PSK / WPA2-PSK, or WPA2-PSK (WPA2-PSK recommended):**

If selecting **WPA-PSK, WPA-PSK / WPA2-PSK, or WPA2-PSK, (Wi-Fi Protected Access Preshared Key)** please review the settings to configure and click **Apply** to save the changes.

Security Configuration	
Security Mode	WPA2
Authentication Type	<input checked="" type="radio"/> PSK <input type="radio"/> EAP
Encryption Type	<input type="radio"/> TKIP <input checked="" type="radio"/> AES <input type="radio"/> TKIP and AES
Group Rekey Time	86400 (seconds)
Passphrase	
Confirmed Passphrase	1234567890

First, from the Security Mode drop-down list, select **WPA-PSK, WPA-PSK / WPA2-PSK, or WPA2-PSK**.

- Select the **Encryption** type. When selecting **WPA-PSK** security, it is recommended to use **TKIP**.
- When selecting **WPA-PSK / WPA2-PSK** security, it is recommended to use **AES**.
- When selecting **WPA2-PSK** security, it is recommended to use **AES**.

Create your Wireless security preshared key (password or key):

- **Preshare Key:** Enter the preshared key.
    - **This is the password or key that is used to connect your computer to this router wirelessly**
- Note:** 8-63 alphanumeric characters (a,b,c,?,\*,/,1,2, etc.)

Then from the PSK/EAP row, select either **PSK or EAP**

- **PSK** stands for Preshared Key
- **EAP** stands for Extensive Authentication Protocol, also called Remote Authentication Dial-In User Service or RADIUS).
 

**Note:** EAP requires an external RADIUS server, PSK only requires you to create a passphrase.

**Selecting WPA, WPA / WPA2, or WPA2:**

If selecting **WPA, WPA / WPA2, or WPA2 (Wi-Fi Protected Access Extensible Authentication Protocol)** please review the settings to configure and click **Apply** to save

WEP Key Format	HEX	ASCII
Character set	0-9 & A-F, a-f only	Alphanumeric (a,b,c,?,*,/,1,2, etc.)
64-bit key length	10 characters	5 characters
128-bit key length	26 characters	13 characters

the changes.

**EAP** (Extensible Authentication Protocol) is also called Remote Authentication Dial-In User Service or RADIUS.

Select the **Encryption** Type

- When selecting **WPA** security, it is recommended to use **TKIP**.
- When selecting **WPA / WPA2** security, it is recommended to use **AES**.
- When selecting **WPA2** security, it is recommended to use **AES**.



Security Configuration	
Security Mode	WPA2
Authentication Type	<input type="radio"/> PSK <input checked="" type="radio"/> EAP
Encryption Type	<input type="radio"/> TKIP <input checked="" type="radio"/> AES <input type="radio"/> TKIP and AES
Group Rekey Time	86400 (seconds)
Radius Server IP	0.0.0.0
Radius Server Port	1812
Radius Server Key	

- **RADIUS Server IP:** Enter the IP address of the RADIUS server. (e.g. 192.168.10.250)
- **RADIUS Port:** Enter the port your RADIUS server is configured to use for RADIUS authentication.

**Note:** It is recommended to use port 1812.

- **RADIUS Shared Key:** Enter the shared key (or shared secret) used to authorize your router with your RADIUS server.

## Connect wireless devices to your router

A variety of wireless network devices can connect to your wireless network such as:

- Gaming Consoles
- Internet enabled TVs
- Network media players
- Smart Phones
- Wireless Laptop computers
- Wireless IP cameras

Each device may have its own software utility for searching and connecting to available wireless networks, therefore, you must refer to the User's Manual/Guide of your wireless client device to determine how to search and connect to this router's wireless network.

See the "Appendix" on [page 59](#) for general information on connecting to a wireless network.

## Connect wireless devices using WPS

Setup > Wireless Settings > WPS Setup

WPS (Wi-Fi Protected Setup) is a feature that makes it easy to connect devices to your wireless network. If your wireless devices support WPS, you can use this feature to easily add wireless devices to your network.

**Note:** You will not be able to use WPS if you set the SSID Broadcast setting to Disabled.

There are two methods the WPS feature can easily connect your wireless devices to your network.

- Push Button Configuration (PBC) method
  - RECOMMENDED Hardware Push Button method—with an external button located physically on your router and on your client device
  - WPS Software/Virtual Push Button - located in router management page
- PIN (Personal Identification Number) Method - located in router management page
 

**Note:** Refer to your wireless device documentation for details on the operation of WPS.

### Recommended Hardware Push Button (PBC) Method

**Note:** it is recommended that a wireless key (passphrase or password) is created before connecting clients using the PBC method. If no wireless key is defined when connecting via PBC, the router will automatically create an encryption key that is 64 characters long. This 64 character key will then have to be used if one has to connect computers to the router using the traditional connection method.

To add a wireless device to your network, simply push the WPS button on the wireless device you are connecting (consult client device User's Guide for length of time), then push and hold the WPS button located on your router for 3 seconds and release it. The WLAN LED on your modem router will flash rapidly indicating that the WPS setup process has been activated. (See "Product Hardware Features" on [page 2](#)) For connecting additional WPS supported devices, repeat this process for each additional device.



**PBC (Software/Virtual Push Button)***Setup > Wireless Settings > WPS Setup*

In addition to the hardware push button located physically on your router, the router management page also has push button which is a software or virtual push button you can click to activate WPS on your router.

1. Log into your router management page (see "Access your router management page" on [page 22](#)).
2. Click on **Setup** and click **Wireless Settings**, then click on the **WPS Setup** button at the bottom of the page.
3. To add a wireless device to your network, simply the push the WPS button on the wireless device (consult wireless device's User's Guide for length of time), you are connecting, then in your router management page, make sure the **Config Method** is set to **Push Button** (default setting) and click on the **Trigger** button at the bottom of the page.

Add Client	
Setup Methods	<input checked="" type="radio"/> Push Button <input type="radio"/> PIN

4. The **WPS Status** area will display status messages about the WPS process.
5. The **WPS Status** area will display "Configured" message to indicate that the wireless client device successfully connected using WPS.

**PIN (Personal Identification Number)***Setup > Wireless Settings > WPS Setup*

If your wireless device has WPS PIN (typically an 8-digit code printed on the wireless device product label or located in the wireless device wireless software utility), you can use this method.

1. Log into your router management page (see "Access your router management page" on [page 22](#)).
2. Click on **Setup** and click **Wireless Settings**, then click on the **WPS Setup** button at the bottom of the page.
3. Next to **Config Status**, click **Release**. The status will change to **Unconfigured**.

Basic Setting	
Enable WPS	<input checked="" type="checkbox"/>
Device Password (PIN)	<input type="text" value="67083985"/> <input type="button" value="Generate New PIN"/> <input type="button" value="Reset PIN to Default"/>
Configuration State	Configured <input type="button" value="Reset to Not-configured"/>
Auto-lock-down State:	Unlocked

4. Click the **Config Method** drop-down list and select **PIN Code**. Click **Apply**.
5. In the empty field, enter the 8-digit WPS PIN of the wireless client device you are connecting and click **Trigger**.

Add Client	
Setup Methods	<input type="radio"/> Push Button <input checked="" type="radio"/> PIN
Client PIN	<input type="text"/>

**Note:** You may need to initiate the WPS PIN on your wireless device first when using this method. Refer to your wireless device documentation for details on the operation of WPS.

6. The **WPS Status** area will display "Configured" message to indicate that the wireless client device successfully connected using WPS.

**Basic wireless settings***Setup > Wireless Settings*

This section outlines available management options under the Wireless Settings tab.

1. Log into your router management page (see "Access your router management page" on [page 22](#)).
2. Click on **Setup**, and click on **Wireless Settings**.
3. To save changes to this section, click **Apply** when finished.

Device Name	wlan0
Device	<input checked="" type="checkbox"/> Enable
SSID	TRENDnet 721
BSSID	00:18:E7:5C:42:E9
Wireless Channel	2437 GHz - CH6
Wireless Mode	802.11n + 802.11g + 802.11b

#### • Device

- **Enable** turns on the wireless networking on your router (by default it is enabled).
- **Disable** turns off wireless networking on your router.

**Note:** It is recommended to leave the wireless setting to **Enable** unless you do not plan on connecting any wireless computers or devices to your network.

- **SSID:** This acronym stands for Service Set Identifier and is the name of your wireless network. It differentiates your wireless network from others around you. By default, the router broadcast TRENDnet721 as the wireless network name. If you choose to change the SSID, change it to a name that you can easily remember.
- **Wireless Channel:** In North America, this router can broadcast on 1 of 11 Channels (13 in Europe and other countries). Selecting the Auto option enables the router to automatically select the best Channel for wireless communication. To manually set the channel on which the router will broadcast, click the drop-down list and select the desired Channel for wireless communication. The goal is to select the Channel that is least used by neighboring wireless networks.
- **Wireless Mode:** Select the appropriate mode for your network.
  - **B/G/N mixed:** Select this mode for the best compatibility. This mode allows older 802.11b and 802.11g wireless devices to connect to the router in addition to newer 802.11n devices.
  - **B/G mixed:** This mode only allows devices to connect to the router using older and slow 802.11b or 802.11g technology and it thereby reduces the router's maximum speed to 54Mbps (typically not recommended).
  - **N only:** This mode only allows newer 802.11n devices to connect to your router. This mode does ensure the highest speed and security for your network, however if you have older 802.11g wireless clients, they will no longer be able to connect to this router.
  - **G only:** This mode only allows devices to connect to the router using older and slow 802.11g technology (typically not recommended).

- **B only:** This mode only allows devices to connect to the router using older and slow 802.11b technology (typically not recommended).

**Note:** Please check the specifications on your wireless devices for the highest wireless capability supported first before applying these settings. If you are unsure, it is recommended that you keep the default setting (B/G/N mixed) for the best compatibility.

When applying the 802.11 mode setting, please keep in mind the following:

- Wireless devices that support 802.11n are backwards compatible and can connect wirelessly at 802.11g or 802.11b.
- Connecting at 802.11b or 802.11g will limit the capability of your 802.11n supported wireless devices from obtaining higher performance and data rates.
- Allowing 802.11b or 802.11g devices to connect to an 802.11n capable wireless network may degrade the wireless network performance below the higher performance and data rates of 802.11n.
- Wireless devices that only support 802.11b or 802.11g will not be able to connect to a wireless network that is set to 802.11n only mode.
- Wireless devices that only support 802.11b will not be able to connect to a wireless network that is set to 802.11g only mode.

## Guest Network

Setup > Wireless Settings

This section outlines available management options under the Wireless Settings tab.

1. Log into your router management page (see "Access your router management page" on [page 22](#)).
2. Click on **Setup**, and click on **Guest Network**.
3. To save changes to this section, click **Apply** when finished.

Guest Network - 2.4GHz	
Radio On/Off	<input checked="" type="checkbox"/>
Name(SSID)	TRENDnet721_2.4GHz_Guest
Security Configuration	
Security Mode	None

- **Radio On/Off:** Select to enable wireless guest network.
- **Name (SSID):** Enter the wireless name or SSID of your guest network.
- **Security Mode:** Select the wireless security or encryption of your guest network.

### Steps to improve wireless connectivity

There are a number of factors that can impact the range of wireless devices. Follow these tips to help improve your wireless connectivity:

1. Keep the number of obstructions to a minimum. Each obstruction can reduce the range of a wireless device. Position the wireless devices in a manner that will minimize the amount of obstructions between them.
  - a. For the widest coverage area, install your router near the center of your home, and near the ceiling, if possible.
  - b. Avoid placing the router on or near metal objects (such as file cabinets and metal furniture), reflective surfaces (such as glass or mirrors), and masonry walls.
  - c. Any obstruction can weaken the wireless signal (even non-metallic objects), so the fewer obstructions between the router and the wireless device, the better.
  - d. Place the router in a location away from other electronics, motors, and fluorescent lighting.
  - e. Many environmental variables can affect the router's performance, so if your wireless signal is weak, place the router in several locations and test the signal strength to determine the ideal position.
2. Building materials can have a large impact on your wireless signal. In an indoor environment, try to position the wireless devices so that the signal passes through less dense material such as dry wall. Dense materials like metal, solid wood, glass or even furniture may block or degrade the signal.
3. Antenna orientation can also have a large impact on your wireless signal. Use the wireless adapter's site survey tool to determine the best antenna orientation for your wireless devices.
4. Interference from devices that produce RF (radio frequency) noise can also impact your signal. Position your wireless devices away from anything that generates RF noise, such as microwaves, radios and baby monitors.

If possible, upgrade wireless network interfaces (such as wireless cards in computers) from older wireless standards to 802.11n. If a wirelessly networked device uses an older standard, the performance of the entire wireless network may be slower. If you are still experiencing low or no signal consider repositioning the wireless devices or installing additional access points.

## Advanced wireless settings

Setup > Wireless Settings

The advanced wireless features can provide you with additional options for setting up your wireless network such as multiple SSID, activate/deactivate wireless according to schedule, and operation modes such as WDS (Wireless Distribution System) bridging or wireless bridging.

### Multiple SSID

Setup > Wireless Settings

The multiple SSID feature allows you to broadcast up to two additional SSIDs (or wireless network names). To wireless devices searching for available wireless networks to connect to, the SSIDs (or wireless network names) will appear as separate and different wireless networks. Since they appear as separate wireless networks, they are also referred to as virtual APs (Access Points). Each virtual AP can be configured each with a different SSID (or wireless network name), security type and additional settings for wireless devices to connect. You can use the multiple SSID feature to setup guest wireless accounts with a different security type to keep your primary wireless network security information private. In addition, the SSIDs can be mapped to a specified VLAN ID. See the VLAN section for instructions on assigning VLAN IDs to the SSIDs.

1. Log into your router management page (see “Access your router management page” on [page 22](#)).
2. Click on **Advanced**, and click on **MBSSID**.
3. Review the settings and click Apply to save settings.

Wireless-Guest/Virtual Access Points			
Enable	SSID(VAP)	BSSID	SSID Advertise
<input type="checkbox"/>	TRENDnet72124C	00:18:E7:5C:42:EA	<input checked="" type="checkbox"/>
<input type="checkbox"/>	WLAN_vap1	00:18:E7:5C:42:EB	<input checked="" type="checkbox"/>
<input type="checkbox"/>	WLAN_vap2	00:18:E7:5C:42:EC	<input checked="" type="checkbox"/>
<input type="checkbox"/>	WLAN_vap3	00:18:E7:5C:42:ED	<input checked="" type="checkbox"/>

- **Enable:** Check box to enable SSID
- **SSID (VAP):** Enter the SSID you would like to apply.
- **BSSID:** MAC address of the SSID

- **SSID Advertise:** Select to broadcast SSID.

4. See section [Secure your wireless network](#) to configure wireless security settings.

### Additional Wireless Settings

Advanced > Advanced Wireless

These settings are advanced options that can be configured to change advanced wireless broadcast specifications. It is recommended that these settings remain set to their default values unless you are knowledgeable about the effects of changing these values. Changing these settings incorrectly can degrade performance.

1. Log into your router management page (see “Access your router management page” on [page 22](#)).
2. Click on **Advanced**, and click on **Advanced Wireless**. Click **Apply** to save settings.

Wireless router settings	
SSID Advertise	<input checked="" type="checkbox"/> Enable
Transmit Power	MAX
Data Rate	Auto Mbps
Fragment Threshold	2346 (256~2346)
RTS Threshold	2347 (0~2347)
Beacon Interval	100 (100~1024ms)
Settings for 11n mode only	
Channel Width	40MHz
20/40MHz Coexist	<input type="checkbox"/> Enable
Legacy Protection	<input type="checkbox"/> Enable
Control Sideband	Lower
Aggregation	<input checked="" type="checkbox"/> Enable
Short GI	<input checked="" type="checkbox"/> Enable

- **SSID Advertise:** Select enable to broadcast the SSID or wireless network name.

- **Regulatory Domain:** The channel region assigned (FCC 1~11 or ETSI 1~13). This setting cannot be modified and is displayed for informational purposes.
- **Transmit Power:** The wireless transmit power can be modified to a lower setting such as 50%, 25%, and 12% if necessary. Lowering the wireless transmit may help to better stabilize the wireless connectivity and reduce the effects of wireless interference in areas where there are several 2.4GHz wireless devices. (Default: 100%)
- **Data Rate:** Select the operating wireless data rate.
- **Fragment Threshold:** Fragmentation in wireless networks is the process of breaking down data communications into smaller data packets in order to improve data efficiency when transferring or receiving data between wireless devices. The fragmentation threshold defines the maximum size of the data packets that are broken down.
- **RTS Threshold:** The Request To Send (RTS) function is part of the networking protocol. A wireless device that needs to send data will send a RTS before sending the data in question. The destination wireless device will send a response called Clear to Send (CTS). The RTS Threshold defines the smallest data packet size allowed to initiate the RTS/CTS function.  
Default Value: 2347 (range: 256-2346)
- **Beacon Interval:** A beacon is a management frame used in wireless networks that transmitted periodically to announce the presence and provide information about the router's wireless network. The interval is the amount time between each beacon transmission.  
Default Value: 100 milliseconds (range: 1-1000)
- **Bandwidth:** This setting only applies to wireless devices connecting at 802.11n. Another term used to describe this parameter is Channel Width. Select the appropriate channel width for your wireless network.
  - **20 MHz:** This mode operates using a single 20MHz channel for wireless devices connecting at 802.11n. This setting may provide more stability than Auto 20/40 MHz for connectivity in busy wireless environments where there are several wireless networks in the area.
  - **Auto 20 MHz/40 MHz:** This mode can automatically switch between using a single 20MHz channel or 40MHz (two 20MHz channels). When 40MHz is active, this mode is capable of providing higher performance only if the wireless devices support the 40MHz channel width. Enabling 20/40MHz typically results in substantial performance increases when connecting to an 802.11n client.

- **20/40MHz Coexist:** Select enable to allow both 20MHz and 40MHz bandwidth connections.
- **Legacy Protection:** Select to enable legacy protection feature.
- **Control Sideband:** Select the side band to use.
- **Aggregation:** Select to enable link aggregation feature.
- **Short GI:** Select to enable short guard interval (400ns).

## Access Control Filters

### Access control basics

#### Wireless MAC address filters

*Advanced > Advanced Wireless > Wireless MAC Filter*

Every network device has a unique, 12-digit MAC (Media Access Control) address. Using wireless MAC filters, you can allow or deny specific wireless clients using this router's wireless network.

1. Log into your router management page (see "Access your router management page" on [page 22](#)).
2. Click on **Advanced**, click on **Advanced Wireless**, and click on **Wireless MAC Filter**.
3. Review the settings and click Apply to save settings.

Wireless Network	
Name (SSID)	media <span>▼</span>
MAC Restrict Mode	<input checked="" type="radio"/> Disable <input type="radio"/> Deny <input type="radio"/> Allow
MAC Address	<input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> <span style="float: right; background-color: #007bff; color: white; padding: 2px 5px; border-radius: 3px;">&lt;&lt; Add</span>

- **Name (SSID):** Select the SSID or wireless network name you would like to apply the wireless MAC filter rule.
- **MAC Restrict Mode:** Select restriction type to use.
- **MAC Address:** Enter the MAC address to apply the rule. Click Add to add MAC address to select rule.

**Note:** Any unspecified MAC/IP addresses or entries without the **Allow** option checked will be denied network access.

## MAC address filters

Advanced > Firewall > MAC Filter

Every network device has a unique, 12-digit MAC (Media Access Control) address. Using MAC filters, you can allow or deny specific computers and other devices from using this router's wired or wireless network.

1. Log into your router management page (see "Access your router management page" on [page 22](#)).
2. Click on **Advanced**, click on **Firewall**, and click on **MAC Filter**.
3. Add the MAC addresses to the MAC Table first before applying the MAC filter function.

Ethernet Interface	
MAC Address	<input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> <input type="button" value=" &lt;&lt; Add"/>
Lan Client	unknow.00:0F:0D:26:40:6E <input type="button" value=" Clone"/>

**Note:** MAC filter can be configured to allow access to the listed MAC address and deny all others unlisted or vice versa. The recommended function is to choose to only allow access to the MAC addresses listed and deny all others unlisted because it is easier to determine the MAC addresses of devices in your network then to determine which MAC addresses you do not want to allow access.

To simplify configuration, click the **LAN clients** drop-down list to select a computer or device that is currently connected to your router. Once you have selected the computer or device, click the **ID** drop-down list to select which entry to copy the selected DHCP client information and click **Clone**. You can choose a DHCP client from the drop down list or you can manually enter the MAC/IP address information.

**Note:** If you are manually entering the MAC/IP address information, refer to your computer or device documentation to find the MAC address.

4. After the MAC address (e.g. 00:11:22:AA:BB:CC) and IP address (e.g. 192.168.10.101) information is entered, make sure the **Allow** option next to the entry to allow network access for this MAC address.
5. Next to **MAC Address Control** at the top of the page, check the **Enable** option to enable MAC filtering. **Note:** Please add MAC/IP address entries first before enabling.

MAC Address Control	<input checked="" type="checkbox"/> Enable
Control Action	<input checked="" type="radio"/> Allow <input type="radio"/> Deny

## URL/Keyword Blocking

Advanced > Firewall > URL Filter

You may want to block computers or devices on your network access to websites using specific keywords (e.g. chat, messenger) or URLs (Uniform Resource Locators).

1. Log into your router management page (see "Access your router management page" on [page 22](#)).
2. Click on **Advanced**, click on **Firewall**, and click on **URL Filter**.
3. Review the settings and click apply to save settings.

URL Filter	<input checked="" type="checkbox"/> Enable
Show Redirect Page	<input checked="" type="checkbox"/> Enable

- **URL Filter:** Check option to enable feature.
  - **Show Redirect Page:** Check option to redirect devices to another website when attempting to access blocked websites.
4. Enter the FQDN or Keyword to block and click Add. Select the time schedule of when to enable the rule or select Always to always block entry.

Add FQDN Rule	<input type="text"/> <input type="button" value=" &lt;&lt; Add"/>
Add Keyword Rule	<input type="text"/> <input type="button" value=" &lt;&lt; Add"/>
Time Schedule	Always <input type="button" value=" New Time Schedule"/>

## Domain Filters

Advanced > Firewall > URL Filter

You may want to allow or block computers or devices on your network access to specific websites (e.g. [www.trendnet.com](http://www.trendnet.com), etc.), also called domains.



1. Log into your router management page (see “Access your router management page” on [page 22](#)).
2. Click on **Advanced**, click on **Firewall**, and click on **Domain Filter**.
3. Under Domain blocking section select Enable.

Domain Blocking	<input checked="" type="checkbox"/> Enable
-----------------	--

4. Enter the website URL to block and click Add. Select the time schedule of when to enable the rule or select Always to always block entry.

Domain	<input type="text"/>	Add
Time Schedule	Always	New Time Schedule

## IP Filtering

*Advanced > Firewall > IP Filter*

You may want to block computers or devices on your network access to your network using IP address.

1. Log into your router management page (see “Access your router management page” on [page 22](#)).
2. Click on **Advanced**, click on **Firewall**, and click on **URL Filter**.
3. Click Add to enter settings.

Name	Status	Source IP	Source Port	Destination IP	Destination Protocol	Protocol Type	Time Schedule	Action
<input type="text"/>								
Add								

4. Review the settings and click Apply to save settings.

IP Filter	<input checked="" type="checkbox"/> Enable
Filter Name	<input type="text"/>
Start Source IP Address	<input type="text"/>
End Source IP Address	<input type="text"/>
Source Port	<input type="text"/> (port or port:port)
Start Destination IP Address	<input type="text"/>
End Destination IP Address	<input type="text"/>
Destination Port	<input type="text"/> (port or port:port)
Protocol Type	TCP/UDP
Time Schedule	Always
New Time Schedule	

- **Enable:** Check to enable rule.
- **Filter Name:** Enter the name of the IP filter rule.
- **Start/End Destination IP Address:** Enter the starting and ending points of the source IP address to filter.
- **Source/Destination Port:** Enter the source and destination ports of the filter IP address.
- **Protocol Type:** Select the protocol to filter of the IP address.
- **Schedule:** Select the schedule to apply the IP filter rule or select Always.

## Packet Filters

You may want specify inbound or outbound access control to allow/deny sources (or Internet IP addresses) to your network from the Internet or from computers or devices on your network to the Internet. Firewall rules may allow for more granular control of specific inbound and outbound access between your network and the Internet. It is recommended that these settings remain set to default unless you are knowledgeable about the effects of changing the firewall rule configuration. It is possible to have undesirable functionality from your router if these settings are improperly modified.

1. Log into your router management page (see “Access your router management page” on [page 22](#)).
2. Click on **Advanced** and click on **Packet Filter**.

3. Under Packet Filter section select Enable and click Apply.

Enable/Disable Packet Filter	
Packet Filter	<input checked="" type="checkbox"/> Enable

## Filter

1. To create a new filter rule. Click Add in the Filters section.

Filters					
Index	Name	Interface	Type	Default Action	Action
<input type="button" value="Add"/>					

2. Review the settings and click Apply to save.

Name	<input type="text"/>
Interface	<input type="text"/>
Type	<input type="text" value="In"/>
Default Action	<input type="text" value="Drop"/>

- **Name:** Enter the name of the filter.
- **Interface:**
- **Type:** Select the type of packets to filter. In for incoming packets and Out to filter outgoing packets Select the interface used for the filter..
- **Default Action:** Select to drop or allow the packets.

## Rules

1. To create a new rule. Click Add in the Rules section.

Rules								
Index	Filter Name	Status	Ether Type	Protocol	Rule Action	Origin	Destination	Action
<input type="button" value="Add"/>								

2. Review the settings and click Apply to save.

Filter Name	<input type="text"/>
Enable	<input type="checkbox"/>
Ether Type	<input type="text" value="IPv4"/> <a href="#">Ether Type Value</a>
Protocol	<input type="text" value="ip"/> <a href="#">Protocol Value</a>
Action	<input type="text" value="Drop"/>
Origin IP Address	<input type="text"/>
Origin Mask	<input type="text"/>
Destination IP Address	<input type="text"/>
Destination Mask	<input type="text"/>
VLAN ID	<input type="text"/> (0-4095)
VLAN Priority	<input type="text"/> (0-7)
VLAN Encapsulation	<input type="text"/> (number or alias)
FQDN	<input type="text"/>
ALG	<input type="text" value="--"/>
IP Option	<input type="text" value="--"/>
DSCP	<input type="text" value="--"/> <a href="#">DSCP Value</a>
Source MAC Address	<input type="text"/>
Destination MAC Address	<input type="text"/>

- **Filter Name:** Select the filter name to apply the rule. Enter the name of the filter.
- **Enable:** Check to enable rule
- **Ether Type:** Select the ether type to apply on the rule.
- **Protocol:** Select the protocol type to apply on the rule.
- **Action:** Select the action to take on the rule
- **Origin/Destination IP:** Enter the IP address of the packets origin and destination
- **Origin/Destination Mask:** Enter the Subnet mask of the packets origin and destination.
- **VLAN ID:** Enter the VLAN ID to apply on the rule
- **VLAN Priority:** Enter the VLAN priority of the packets
- **VLAN Encapsulation:** Enter the encapsulation type
- **FQDN:** Enter the domain name
- **ALG:** Select the ALG type
- **IP Option:** Select IP option type



- **DSCP:** Select the DSCP value to apply
- **Source/Destination MAC Address:** Enter the source and destination MAC address of the rule.

### Generic Rules

1. To create a new rule. Click Add in the Rules section.

Index	Filter Name	Status	Type	Protocol	Position	Condition	Value	Rule Action	Action
<input type="button" value="Add"/>									

2. Review the settings and click Apply to save.

Filter Name	<input type="text"/>
Enable	<input type="checkbox"/>
Type	hexadecimal
Proto	IP Header
Position	<input type="text"/>
condition	eq
Value	<input type="text"/>
Action	Drop

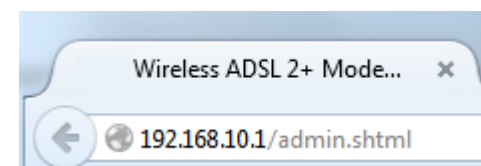
- **Filter Name:** Select the filter name to apply the rule. Enter the name of the filter.
- **Enable:** Check to enable rule
- **Type:** Select the value type to apply on the rule.
- **Proto:** Select the IP Protocol data type
- **Position:** Specify the location of the packet location
- **Condition:** Select the condition type of the rule
- **Value:** Enter the IP checksum value of the packet
- **Action:** Select the action to take of the rule.

## Advanced Router Setup

### Access your router management page

**Note:** Your router management page <http://192.168.10.1> is accessed through the use of your Internet web browser (e.g. Internet Explorer, Firefox, Chrome, Safari, Opera) and will be referenced frequently in this User's Guide.

1. Open your web browser (e.g. Internet Explorer, Firefox, Safari, Chrome, or Opera) and go to <http://192.168.10.1>. Your router will prompt you for a user name and password.



2. Enter the default user name and password and then click Login.

Default User Name: **admin**

Default Password: **xxxxxxxxxx**

Login to the TEW-721BRM	
User Name:	<input type="text"/>
Password:	<input type="password"/>
Language:	English
<input type="button" value="Login"/>	

## Change your router login password

Maintenance > Password

1. Log into your router management page (see “Access your router management page” on [page 22](#)).
2. Click on **Maintenance**, and click on **Password**.
3. Select the user name to apply changes to. In the **Current Password** field, enter the current password. **New Password** field, enter the new password and in the **Confirm** field, retype the new password again to confirm.

Password	
User Name	admin ▼
Current Password	<input type="password"/>
New Password	<input type="password"/>
Confirm Password	<input type="password"/>

4. Click **Apply** at the bottom of the page to save the changes.

**Note:** If you change the router login password, you will need to access the router management page using the User Name “admin” and the new password instead of the default password “admin”.

## Set your router date and time

Setup > Time and Date

There are two ways to set the router's date and time. NTP (Network Time Protocol) is based on time servers. You can also manually set the router's date and time.

**Note:** It is important that the time is configured correctly before setting any schedules. Our router management page <http://192.168.10.1> is accessed through the use of your Internet web browser (e.g. Internet Explorer, Firefox, Chrome, Safari, Opera) and will be referenced frequently in this User's Guide.

1. Log into your router management page (see “Access your router management page” on [page 22](#)).
2. Click on **Setup**, and click on **Time and Date**.
3. Next to **Time Zone**, click the drop-down list to select your time zone.

Time Setting	
Time Zone	(GMT-05:00) Eastern Time (US & Canada) ▼

### NTP

1. Review the settings below and click Apply to save settings.

NTP	
Enable	<input type="checkbox"/>
Server 1 IP or Domain name	pool.ntp.org
Server 2 IP or Domain name	time.windows.com
First Poll Frequency	5 (seconds)
Thereafter Frequency	▼ (minutes)

- **Enable:** Check option to enable NTP feature
- **Server IP:** Enter the NTP server IP address or domain to use.
- **First Poll Frequency:** Enter the initial time to check NTP
- **Thereafter Frequency:** Select the time of when the router will continue to check for NTP updates.

When using NTP time settings you may also configure Daylight Saving feature.

Daylight Saving	
Enable	<input type="checkbox"/>
Start Time	<input type="text"/> <input type="text"/>
End Time	<input type="text"/> <input type="text"/>

- **Enable:** Check option to enable daylight savings
- **Start/End Time:** Configure the start and end time of daylight savings.

### Manual

1. Manually set the date and time of the router by select the from the pull down menus. Click **Sync Time** to synchronize with your computer's current time.

Manually Set Time					
Year	<input type="text" value="2014"/>	Month	<input type="text" value="Oct"/>	Day	<input type="text" value="17"/>
Hour	<input type="text" value="17"/>	Minute	<input type="text" value="04"/>	Second	<input type="text" value="03"/>

- **Year:** Enter the year to **Enable:** Check option to enable NTP feature
- **Server IP:** Enter the NTP server IP address or domain to use.
- **First Poll Frequency:** Enter the initial time to check NTP
- **Thereafter Frequency:** Select the time of when the router will continue to check for NTP updates.

## Manually configure your Internet connection

### Setup > Internet Setup

1. Log into your router management page (see "Access your router management page" on [page 22](#)).
2. Click on **Setup**, and click on **Internet Setup**.
3. Review and configure your Internet connection settings. Click Apply to save settings.

**Note:** Please contact your ISP to determine all configuration settings.

### Internet Connection Settings

Internet Connection Settings	
Profile Name	<input type="text" value="pvc0_8_35"/>
WAN Link Type	<input checked="" type="radio"/> ADSL
ATM Connection	<input type="text" value="PVC 0"/>
Enable	<input type="text" value="Enable"/>
Enable AutoPVC	<input type="text" value="Disable"/>
VPI	<input type="text" value="0"/> (0~255)
VCI	<input type="text" value="35"/> (32~65535)
Encapsulation	<input type="text" value="LLC"/>
ATMQoS	<input type="text" value="UBR"/>
Peak Cell Rate	<input type="text" value="6000"/> (0~6000 cells/s)
Backupid VLAN ID	<input type="text" value="0"/> (0~4095)
Enable Default Vlan	<input type="text" value="Disable"/>
PPPoE Passthrough	<input type="text" value="Disable"/>

- **Profile Name:** Enter the profile name of your connection.
- **WAN Link Type:** Select the WAN link connection type (ADSL)
- **ATM Connection:** Select the Permanent Virtual Circuit (PVC) that will be configured.
- **Enable:** Select enable to activate internet connection.
- **Enable AutoPVC:** Select whether to enable or disable AutoPVC connection.
- **VPI:** Enter your ISP's VPI (Virtual Path Identifier) values
- **VCI:** Enter your ISP's VCI (Virtual Channel Identifier) values.
- **Encapsulation:** Select your ISP's encapsulation settings.
- **ATMQoS:** Select the type of ATM Queue of Service used by your ISP.
- **Peak Cell Rate:** Set the maximum rate of cells provided by your ISP
- **Backup VLAN ID:** Set the backup VLAN ID
- **Enable Default VLAN:** Select enable to activate VLAN
- **PPPoE Passthrough:** Select to enable PPPoE Passthrough.

## Internet Settings

Internet Settings
<input checked="" type="radio"/> PPPoE (RFC-2516 PPP over Ethernet)
<input type="radio"/> PPPoA (RFC-2364 PPP over ATM)
<input type="radio"/> IPoA (RFC-1483 Routed)
<input type="radio"/> Dynamic IP Address (IPoEoA/MER(MAC Encapsulated Routed) with DHCP)
<input type="radio"/> Static IP Address
<input type="radio"/> Bridge Mode (RFC-1483 Bridged)
<input type="radio"/> CIP (RFC-1577 Classic IP/ARP over ATM)

- **Internet Settings:** Select your ADSL internet type. Contact your ISP for additional information.

## PPPoE / PPPoA

If you select PPPoE (RFC-2516 PPP over Ethernet), the screen below is displayed.

PPPoE (RFC-2516 PPP over Ethernet)	
State of Connection	Enable
IP Protocol Version	<input type="radio"/> IPv4 only <input checked="" type="radio"/> IPv4/v6 both <input type="radio"/> IPv6 only
IPMode of Connection	Dynamic
Name	pppoe
NAT	Enable
User Name	8000493@bzn
User Password	*****
Confirm Password	*****
Max MRU	1492 (576~1492)
DNS Enabled	Enable
DNS Override Allowed	Disable
DNS Server 1	(optional)
DNS Server 2	(optional)
PPPoE Service Name	(optional)
MAC Address	00 : 18 : E7 : 5C : 42 : E9 <a href="#">Clone MAC</a>
PPPoE AC Name	(optional)
Connection Trigger	AlwaysOn
Idle Disconnect Time	300 30~3600 seconds
LCP Interval	20 (0~86400 seconds)
As system default route	<input checked="" type="checkbox"/> (Current setting: pppoe)
ICMP Reply Enable	<input checked="" type="checkbox"/>
Proxy ARP Enable	<input type="checkbox"/>

- **State of Connection:** Select whether to enable or disable this connection.
- **IPMode of Connection:** Select the connection mode, options are:

- **Dynamic:** Select this option if the IP address can be automatically obtained from your ISP.
- **Static:** Select this option if you are required to use a permanent IP address to connect to the Internet. You must enter the IP address and subnet mask provided by your ISP.
- **Name:** Enter your desired connection name.
- **NAT:** Select whether to enable or disable NAT (Network Address Translation). Enable this setting to share one WAN IP address with multiple computers on your network.
- **User Name:** Enter the user name provided by your ISP.
- **User Password:** Enter the password provided by your ISP.
- **Confirm Password:** Re-enter the password.
- **Max MRU:** Set the maximum rate of cells that you can receive. If provided by your ISP, enter the rate in the field. Otherwise, leave this field to its default setting.
- **DNS Enabled:** Select whether to enable or disable DNS (Domain Name System).
- **DNS Override Allowed:** Select whether to enable or disable DNS override.
- **DNS Server 1 / DNS Server 2:** If provided by your ISP, enter the DNS server. Otherwise, leave these fields blank.
- **PPPoE Service Name:** Enter a PPPoE service name.
- **MAC Address:** Display the cloned MAC address. Click Clone MAC to clone the MAC address of your computer.
- **PPPoE AC Name:** Enter the PPPoE account name provided by your ISP.
- **Connection Trigger:** Configure how you want your modem router to connect and terminate the Internet connection. Options are:
  - **OnDemand:** Enables the modem router to cut off the Internet connection after being idle for a specified period of time. The device automatically re-establishes the connection when you try to access the Internet again. In the Idle Disconnect Time field, enter the number of seconds that you want to elapse before your modem router terminates the Internet connection.
  - **AlwaysOn:** Enables the modem router to be connected to the Internet at all times. If you are disconnected, the device will automatically re-establish the connection.
  - **Manual:** Manually configure this setting. Enter the user name and password to establish the Internet connection.
- **Idle Disconnect Time:** View the preset idle time before the session is disconnected.
- **LCP Interval:** Enter the number of seconds that you want to be the interval in sending LCP (Link Control Protocol) packets.

- **As system default route:** Check this box to set the current setting as the default route.
- **ICMP Reply Enable:** Check this box to enable ICMP (Internet Control Message Protocol) messages to be sent back to the host that sent the message.
- **Proxy ARP Enable:** Check this box to enable proxy ARP function.

## IPoA

If you select IPoA, the screen below is displayed.

IPoA (RFC-1483 Routed)	
State of Connection	Enable ▾
IP Protocol Version	<input type="radio"/> IPv4 only <input checked="" type="radio"/> IPv4/v6 both <input type="radio"/> IPv6 only
Name	<input type="text"/>
NAT	Enable ▾
External IP Address	<input type="text" value="0.0.0.0"/>
Subnet Mask	<input type="text" value="255.255.255.0"/>
Default Gateway	<input type="text" value="0.0.0.0"/>
DNS Enabled	Enable ▾
DNS Override Allowed	Disable ▾
DNS Server 1	<input type="text"/> (optional)
DNS Server 2	<input type="text"/> (optional)
As system default route	<input type="checkbox"/> (Current setting: pppoe)
ICMP Reply Enable	<input type="checkbox"/>
Proxy ARP Enable	<input type="checkbox"/>

- **State of Connection:** Select whether to enable or disable this connection.
- **Name:** Enter your desired connection name.
- **NAT:** Select whether to enable or disable NAT (Network Address Translation). Enable this setting to share one WAN IP address with multiple computers on your network.
- **External IP Address:** Enter the IP address provided by your ISP.
- **Subnet Mask:** Enter the subnet mask provided by your ISP.

- **Default Gateway:** Enter the default gateway provided by your ISP.
- **DNS Enabled:** Select whether to enable or disable DNS (Domain Name System).
- **DNS Override Allowed:** Select **whether to enable or disable DNS override**.
- **DNS Server 1 / DNS Server 2:** If provided by your ISP, enter the DNS server. Otherwise, leave these fields blank.
- **As system default route:** Check this box to set the current setting as the default route.
- **ICMP Reply Enable:** Check this box to enable ICMP (Internet Control Message Protocol) messages to be sent back to the host that sent the message.
- **Proxy ARP Enable:** Check this box to enable proxy ARP function.

### Dynamic / Static

If you select Dynamic IP, the screen below is displayed.

Dynamic IP Address (IPoEoA/MER(MAC Encapsulated Routed) with DHCP)	
State of Connection	Enable
IP Protocol Version	<input type="radio"/> IPv4 only <input checked="" type="radio"/> IPv4/v6 both <input type="radio"/> IPv6 only
Name	<input type="text"/>
NAT	Enable
DNS Enabled	Enable
DNS Override Allowed	Disable
DNS Server 1	<input type="text"/> (optional)
DNS Server 2	<input type="text"/> (optional)
MAC Address	00 : 18 : E7 : 5C : 42 : E9 <a href="#">Clone MAC</a>
Option 125	Disable
Option 60 Vendor ID	<input type="text"/> (optional)
Option 61 IAID	<input type="text"/> (optional)
Option 61 DUID	<input type="text"/> (optional)
As system default route	<input type="checkbox"/> (Current setting: pppoe)
ICMP Reply Enable	<input type="checkbox"/>
Proxy ARP Enable	<input type="checkbox"/>
Unicast DHCP-Request	<input type="checkbox"/>

- **State of Connection:** Select whether to enable or disable this connection.
- **IP Protocol Version:** Select the IP protocol version.
- **Name:** Enter your desired connection name.
- **NAT:** Select whether to enable or disable NAT (Network Address Translation). Enable this setting to share one WAN IP address with multiple computers on your network.
- **DNS Enabled:** Select whether to enable or disable DNS (Domain Name System).
- **DNS Override Allowed:** Select whether to enable or disable DNS override.
- **DNS Server 1 / DNS Server 2:** If provided by your ISP, enter the DNS server. Otherwise, leave these fields blank.
- **MAC Address:** Displays the cloned MAC address. Click Clone MAC to clone the MAC address of your computer.
- **Option 125:** Select whether to enable or disable Option 125.
- **Option 60 Vendor ID:** Enter option 60 vendor ID.
- **Option 61 IAID:** Enter option 61 IAID.
- **Option 61 DUID:** Enter option 61 DUID.
- **As system default route:** Check this box to set the current setting as the default route.
- **ICMP Reply Enable:** Check this box to enable ICMP (Internet Control Message Protocol) messages to be sent back to the host that sent the message.
- **Proxy ARP Enable:** Check this box to enable proxy ARP function.
- **Unicast DHCP-Request:** Check this box to enable unicast DHCP request function.

### Bridge Mode

If you select Bridge mode, the screen below is displayed.

Bridge Mode (RFC-1483 Bridged)	
State of Connection	Enable
IP Protocol Version	<input type="radio"/> IPv4 only <input checked="" type="radio"/> IPv4/v6 both <input type="radio"/> IPv6 only
Name	<input type="text"/>

- **State of Connection:** Select whether to enable or disable this connection.
- **IP Protocol Version:** Select the IP protocol version.
- **Name:** Enter your desired connection name.

**CIP**

If you select CIP mode, the screen below is displayed.

CIP (RFC-1577 Classic IP/ARP over ATM)	
State of Connection	Enable
IP Protocol Version	<input type="radio"/> IPv4 only <input checked="" type="radio"/> IPv4/v6 both <input type="radio"/> IPv6 only
Name	
NAT	Enable
External IP Address	0.0.0.0
Subnet Mask	255.255.255.255
Default Gateway	0.0.0.0
DNS Enabled	Enable
DNS Override Allowed	Disable
DNS Server 1	(optional)
DNS Server 2	(optional)
As system default route	<input type="checkbox"/> (Current setting: pppoe)
ICMP Reply Enable	<input type="checkbox"/>
Proxy ARP Enable	<input type="checkbox"/>

- **State of Connection:** Select whether to enable or disable this connection.
- **IP Protocol Version:** Select the IP protocol version.
- **Name:** Enter your desired connection name.
- **NAT:** Select whether to enable or disable NAT (Network Address Translation). Enable this setting to share one WAN IP address with multiple computers on your network.
- **External IP Address:** Enter the IP address provided by your ISP.
- **Subnet Mask:** Enter the subnet mask provided by your ISP.
- **Default Gateway:** Enter the default gateway provided by your ISP.
- **DNS Enabled:** Select whether to enable or disable DNS (Domain Name System).
- **DNS Override Allowed:** Select whether to enable or disable DNS override.
- **DNS Server 1 / DNS Server 2:** If provided by your ISP, enter the DNS server. Otherwise, leave these fields blank.

- **As system default route:** Check this box to set the current setting as the default route.
- **ICMP Reply Enable:** Check this box to enable ICMP (Internet Control Message Protocol) messages to be sent back to the host that sent the message.
- **Proxy ARP Enable:** Check this box to enable proxy ARP function.

## Change your router IP address

Setup > Local Network

In most cases, you do not need to change your router IP address settings. Typically, the router IP address settings only needs to be changed, if you plan to use another router in your network with the same IP address settings, if you are connecting your router to an existing network that is already using the IP address settings your router is using, or if you are experiencing problems establishing VPN connections to your office network through your router.

**Note:** If you are not encountering any issues or are not faced with one of the cases described above or similar, it is recommended to keep your router IP address settings as default.

Default Router IP Address: 192.168.10.1

Default Router Network: 192.168.10.0 / 255.255.255.0

1. Log into your router management page (see "Access your router management page" on [page 22](#)).
2. Click on **Setup**, and click on **Local Network**.
3. Review the settings and click **Apply** to save changes.

LAN	
IP Address	192.168.10.1
Subnet Mask	255.255.255.0
Local Domain Name	(optional)
DNS Relay	<input checked="" type="checkbox"/> Enable

- **LAN IP Address:** Enter the new router IP address. (e.g. 192.168.200.1)



**Note:** You will need to access your router management page using your new router IP address to access the router management page. (e.g. Instead of using the default <http://192.168.10.1> using your new router IP address will use the following format using your new router IP address [http://\(new.router.ipaddress.here\)](http://(new.router.ipaddress.here)) to access your router management page.

- **Subnet Mask:** Click the Subnet Mask drop-down list to select a mask. (e.g. 255.255.255.0)
- **Local Domain Name:** Enter the domain name to assign your router.
- **DNS Relay:** Select enable to activate DNS relay

**Note:** The DHCP address range will change automatically to your new router IP address settings so you do not have to change the DHCP address range manually to match your new router IP address settings.

## Set up the DHCP server on your router

### Setup > Local Network

Your router can be used as a DHCP (Dynamic Host Configuration Protocol) server to automatically assign an IP address to each computer or device on your network. The DHCP server is enabled by default on your router. If you already have a DHCP server on your network, or if you do not want to use your router as a DHCP server, you can disable this setting. It is recommended to leave this setting enabled.

1. Log into your router management page (see "Access your router management page" on [page 22](#)).
2. Click on **Setup**, and click on **Local Network**.
3. Review the DHCP Server settings.

DHCP setting	
DHCP Option	<input type="radio"/> Disable <input checked="" type="radio"/> DHCP Server <input type="radio"/> DHCP Relay
IP Pool Starting Address	192.168.10.101
IP Pool Ending Address	192.168.10.200
Subnet Mask	255.255.255.0
Router IP Address	192.168.10.1
Primary DNS Servers	192.168.10.1
Secondary DNS Servers	
Lease Time	86400 (seconds)
Sub Range IP Enable	<input type="checkbox"/>
Extra Option Enable	<input type="checkbox"/>

- **DHCP Option:** Select the DHCP mode of your modem router. If you set the DHCP Option to DHCP Server, configure the following settings:  
**Note:** If you set your modem router as the DHCP server, your modem router will automatically assign an IP address to each computer on your network. By default, the fields for DHCP settings have predefined values. It is recommended to retain these values unless specified by your ISP.
- **IP Pool Starting Address:** Enter the lowest range of IP address to assign. The default value is 192.168.10.101.
- **IP Pool Ending Address:** Enter the highest range of IP address to assign. The default value is 192.168.10.200.
- **Subnet Mask:** Enter the subnet mask. The default value is 255.255.255.0.
- **Router IP Address:** Enter the IP address of your modem router. The default value is 192.168.10.1.
- **Primary DNS Servers / Secondary DNS Servers:** Enter a primary and a secondary DNS server if the DNS Relay option is enabled.
- **Lease Time:** Enter the lease time in seconds. The lease time is the amount of time a device is allowed connection to your modem router using its current dynamic IP address. At the end of the lease time, the lease is either renewed or a new IP address is assigned. The default value is 86400 seconds (1 day).



- **Sub Range IP Enable:** Check this box to set another range of IP address.
- **Vendor Class (Option 60):** Enter a vendor class name.
  - **Sub-String Match:** Check to enable the sub-string match function.
  - **IP Pool Starting Address:** Enter the lowest sub range of IP address to assign.
  - **IP Pool Ending Address:** Enter the highest sub range of IP address to assign.
  - **Subnet Mask:** Enter the subnet mask.
  - **IP Routers:** Enter the IP address of your modem router.
  - **Primary DNS Servers / Secondary DNS Servers:** Enter a primary and a secondary DNS server of the sub range.
- **Extra Option Enable:** Check this box to enable extra options. If you set the DHCP Option to DHCP Relay, configure the following settings:  
***Note:** Some ISPs function as the DHCP server for their clients' small office network. In this case, you can set your modem router to act as a DHCP relay agent. When a device on your network requests Internet access, your modem router contacts the ISP to obtain the*

## Enable/disable UPnP on your router

Advanced > UPnP

UPnP (Universal Plug and Play) allows devices connected to a network to discover each other and automatically open the connections or services for specific applications (e.g. instant messenger, online gaming applications, etc.) UPnP is enabled on your router by default to allow specific applications required by your computers or devices to allow connections through your router as they are needed.

1. Log into your router management page (see "Access your router management page" on [page 22](#)).
2. Click on **Advanced**, and click on **UPnP**.
3. Review the settings and click **Apply** to save settings.

UPnP	<input checked="" type="checkbox"/> Enable
UPnP LOG	<input checked="" type="checkbox"/> Enable
TR064	<input checked="" type="checkbox"/> Enable

- **UPnP:** Select this option to enable UPnP
- **UPnP Log:** Select this option to activate UPnP log and status
- **TR064:** Select this to option to enable TR064 feature.

**Note:** It is recommended to leave this setting enabled, otherwise, you may encounter issues with applications that utilize UPnP in order allow the required communication between your computers or devices and the Internet.

## Allow/deny VPN connections through your router

Advanced > NAT > VPN Passthrough

A Virtual Private Network (VPN) is a network that uses a public network, such as the Internet, to provide secure communications between a remote computer or network and another network. Some offices often provide VPN access to their networks to enable employees to work from their remote office/home office, or while traveling. If your office or place of work has allowed and authorized access for you to access their network through VPN, the default VPN settings in your router have been configured to pass through the most common types of VPN protocols, which typically do not require any additional configuration changes.

1. Log into your router management page (see "Access your router management page" on [page 22](#)).
2. Click on **Advanced**, click on **NAT**, and click on **Passthrough**.
3. Review the settings and click **Apply** to save settings.

IPSEC Passthrough	<input checked="" type="checkbox"/> Enable	IPSEC Port:	500 (UDP)
PPTP Passthrough	<input checked="" type="checkbox"/> Enable	PPTP Port:	1723 (TCP)
L2TP Passthrough	<input checked="" type="checkbox"/> Enable	L2TP Port:	1701 (UDP)

- **IPSEC Passthrough:** Internet Protocol Security (IPSec) is a protocol suite used to secure IP communications by authenticating and encrypting IP packets. Check this box to enable this function to work through your modem router.
- **PPTP Passthrough:** Point-to-Point Tunneling Protocol (PPTP) allows Point-to-Point protocol (PPP) to be tunneled through a network. Check this box to enable this function to work through your modem router.
- **L2TP Passthrough:** Layer 2 Tunneling Protocol (L2TP) is an extension to the PPP protocol that enables ISPs to operate VPNs.

**Note:** It is recommended to leave these settings unchecked to ensure VPN passthrough capability is enabled on your router.

## Configure ALG settings

Advanced > NAT > ALG

A Virtual Private Network (VPN) is a network that uses a public network, such as the Internet, to provide secure communications between a remote computer or network and another network. Some offices often provide VPN access to their networks to enable employees to work from their remote office/home office, or while traveling. If your office or place of work has allowed and authorized access for you to access their network through VPN, the default VPN settings in your router have been configured to pass through the most common types of VPN protocols, which typically do not require any additional configuration changes.

1. Log into your router management page (see "Access your router management page" on [page 22](#)).
2. Click on **Advanced**, click on **NAT**, and click on **ALG**.
3. Review the settings and click **Apply** to save settings.

FTP	<input checked="" type="checkbox"/> Enable	FTP Port:	21 (TCP)		
SNMP	<input checked="" type="checkbox"/> Enable	SNMP Port:	161 (UDP)	TRAP Port:	162 (UDP)
RTSP	<input checked="" type="checkbox"/> Enable	RTSP Port:	554 (TCP)		
SIP	<input checked="" type="checkbox"/> Enable	SIP Port:	5060 (UDP)		
IRC	<input checked="" type="checkbox"/> Enable	IRC Port:	6667 (TCP)		
H323	<input checked="" type="checkbox"/> Enable	RAS Port:	1719 (UDP)	Q931 Port:	1720 (TCP)

- **FTP:** File Transfer Protocol (FTP) is used to transfer files between computers on a TCP/IP based network, such as the Internet. Check this box to enable this function to work through your modem router.
- **SNMP:** Simple Network Management Protocol (SNMP) is a network protocol used to monitor the devices connected to a network. Check this box to enable this function to work through your modem router.
- **RTSP:** Real Time Streaming Protocol (RTSP) is a network protocol used for entertainment and communication systems to control streaming media sessions. Check this box to enable this function to work through your modem router.
- **SIP:** Session Initiation Protocol (SIP) is a signaling protocol used to control multimedia communication sessions such as voice and video calls over Internet

Protocol (IP). Check this box to enable this function to work through your modem router.

- **IRC:** Internet Relay Chat (IRC) is a real-time Internet chatting protocol designed for group communications. Check this box to enable this function to work through your modem router.
- **H323:** H.323 is a standard that provides audio-visual communication sessions on a network. It is widely implemented in voice and video conferencing equipments and is used within various Internet real-time applications such as NetMeeting. Check this box to enable this function to work

## Additional Security Settings

Advanced > Firewall

To provide additional security, your router offers DoS (Denial of Service) detection and SPI mode further prevent network attacks. You may want to enable these features for additional network security.

### DoS Protection

1. Log into your router management page (see "Access your router management page" on [page 22](#)).
2. Click on **Advanced**, click on **Firewall**, and click on **DoS Protection**.
3. Review the settings below and click Apply to save settings.

Dos Protection	<input checked="" type="checkbox"/> Enable
Dos Protection Option	Type -- Support Whole_System flood, Per-Source flood, and other Dos Protection type Enable -- Enable/Disable this kind of Dos Protection Count -- Input flood count number of this kind of Dos Protection (0~65535 packets/seconds).
Whole_Sys SYN Flood	<input type="checkbox"/> Flood Count(0~65535 packets) 100
Whole_Sys FIN Flood	<input type="checkbox"/> Flood Count(0~65535 packets) 100
Whole_Sys UDP Flood	<input type="checkbox"/> Flood Count(0~65535 packets) 100
Whole_Sys ICMP Flood	<input type="checkbox"/> Flood Count(0~65535 packets) 100
Per_Src IP SYN Flood	<input type="checkbox"/> Flood Count(0~65535 packets) 100
Per_Src IP FIN Flood	<input type="checkbox"/> Flood Count(0~65535 packets) 100

- **Dos Protection:** Check this box to enable DoS protection.
- **Dos Protection Option:** Check the appropriate boxes to enable protection from SYN flood, FIN flood, UDP flood, ICMP flood, SMURF, IP spoofing, and others. Enter the flood count numbers or retain the default values if you are unsure about them.

### SPI Settings

1. Log into your router management page (see "Access your router management page" on [page 22](#)).
2. Click on **Advanced**, click on **Firewall**, and click on **SPI Settings**.
3. Review the settings below and click Apply to save settings.

SPI Enable	Enable ▾
Endpoint Filter	restrict ▾
Log Dropped Packet Enable	Disable ▾

- **SPI Enable:** Select whether to enable or disable the SPI function.
- **Endpoint Filter:** Select an endpoint filter option:
  - **Independent:** Forwards all incoming traffic from an open port to the application that opened the port.
  - **Restrict:** Incoming traffic must match the IP address of the outgoing connection.
- **Log Dropped Packet Enable:** Select whether to enable or disable logging of dropped packets from your network or the Internet.

## Allow/deny multicast streaming

### Setup > Internet Setup

In some cases, applications require multicast communication (also called IP multicast which is the delivery of information to a specific group of computers or devices in a single transmission) typically used in media streaming applications. Multicast streaming is disabled by default on your router to deny applications that require multicast communication through your router.

### IGMP

1. Log into your router management page (see "Access your router management page" on [page 22](#)).

2. Click on **Advanced**, click on **Multicast** and select **IGMP**.
3. Under IGMP option select which IGMP to activate.

IGMP Option    ☒ Disable   ☐ Proxy   ☐ Snooping

3. Review the settings below and click Apply to save changes.

### IGMP Proxy /Snooping

IGMP Option	<input type="radio"/> Disable <input checked="" type="radio"/> Proxy <input type="radio"/> Snooping
IGMP Proxy Version	IGMPv2 ▾
DSL Interface	ppoe ▾
Connected Interfaces	
IGMP Fast Leave	<input type="checkbox"/>
IGMP Query Interval	30 (1~250seconds)
Robust Count	3 (1~10)
IGMP Last Member Query Interval	3 (1~250seconds)
IGMP Robustness	2 (1~10)
Query Response Interval	10 (1~10 100milliseconds)
Group Live Delay Time	1 (0~100 100milliseconds)
WLAN	<input checked="" type="checkbox"/> Enable IGMP
LAN1	<input checked="" type="checkbox"/> Enable IGMP
LAN2	<input checked="" type="checkbox"/> Enable IGMP
LAN3	<input checked="" type="checkbox"/> Enable IGMP
LAN4	<input checked="" type="checkbox"/> Enable IGMP

- **IGMP Proxy Version:** Select IGMP version to activate
- **DSL Interface:** Select the interface to set
- **IGMP Fast Leave:** Select option to enable fast leave feature
- **IGMP Query Interval:** Enter IGMP query interval
- **Robust Count:** Enter robust count
- **IGMP Last Member Query Interval:** Enter last member query interval
- **IGMP Robustness:** Enter robustness value
- **Query Response Interval:** Enter response interval
- **Group Live Delay Time:** Enter group live delay time

- **WLAN/LAN1-4:** Select device interface to reflect IGMP rule.

### MLD

1. Log into your router management page (see “Access your router management page” on [page 22](#)).
2. Click on **Advanced**, click on **Multicast** and select **IGMP**.
3. Under MLD option select which IGMP to activate.

MLD Option	<input checked="" type="radio"/> Disable <input type="radio"/> Proxy <input type="radio"/> Snooping
------------	---

3. Review the settings below and click Apply to save changes.

### MLD Proxy /Snooping

MLD Option	<input type="radio"/> Disable <input checked="" type="radio"/> Proxy <input type="radio"/> Snooping	
DSL Interface	pppoe ▼	
Connected Interfaces		
Fast Leave	<input type="checkbox"/>	
Query Interval	125	(10~65535 .seconds)
Robust Count	2	(1~15)
Last Member Query Interval	1000	(1000~32767 milliseconds.)
Last Member Query Count	2	(1~15)
Query Response Interval	10000	(1000~65535 milliseconds.)

- **DSL Interface:** Select the interface to set
- **Fast Leave:** Select option to enable fast leave feature
- **Query Interval:** Enter IGMP query interval
- **Robust Count:** Enter robust count
- **Last Member Query Interval:** Enter last member query interval
- **Last Member Query Count:** Enter last member query count
- **Query Response Interval:** Enter response interval

## Identify your network on the Internet

### Advanced > Dynamic DNS

Since most ISPs constantly change your home IP address, providing access to devices on your home or small office Local Area Network (such as IP Cameras) from the Internet requires setting up a Dynamic DNS service and entering the parameters into this management area. Dynamic DNS services allow your router to confirm its location to the given Dynamic DNS service, thereby providing the Dynamic DNS service with the ability to provide a virtual fixed IP address for your network. This means that even though your ISP is always changing your IP address, the Dynamic DNS service will be able to identify your network using a fixed address—one that can be used to view home IP Camera and other devices on your local area network.

**Note:** First, you will need to sign up for one of the DDNS service providers listed in the **Server Address** drop-down list.

1. Sign up for one of the DDNS available service providers list under **Server Address**. (e.g. *dyndns.com*, *no-ip.com*, etc.)
2. Log into your router management page (see “Access your router management page” on [page 22](#)).
3. Click on **Advanced** and click on **Dynamic DNS**.
4. Next to DDNS, click **Enable**.

Connection Name	pppoe ▼
Use Dynamic DNS Service	<input checked="" type="checkbox"/> Enable
Service Provider	dyndns.org ▼
Host Name	
User Name	
Password	
Confirm Password	
Use Wildcards	<input type="checkbox"/> Enable

5. In the **Server Address** drop-down list, select the provider you selected, and enter your information in the fields.

- **Host Name:** Personal URL provided to you by your Dynamic DNS service provider (e.g. *www.trendnet.dyndns.biz*)

- **User Name / E-mail:** The user name needed to log in to your Dynamic DNS service account
- **Password/Key:** This is the password to gain access to Dynamic DNS service (NOT your router or wireless network password) for which you have signed up to.

6. To save changes, click **Apply**.

## Allow remote access to your router management page

*Maintenance > Remote Management*

You may want to make changes to your router from a remote location such as at your office or another location while away from your home.

1. Log into your router management page (see "Access your router management page" on [page 22](#)).
2. Click on **Maintenance**, and click on **Remote Management**.
3. Under the **Only allow administrator access from WAN** section, click **Enabled** and click **Apply** to save settings.

Only allow administrator access from WAN. ☒

### Http Management

Http Enable :	<input type="checkbox"/>
HTTP WAN Port :	<input type="text" value="32521"/>
Session Timeout :	<input type="text" value="10"/> 1~1440 Minutes

- **Http Enable:** Select to enable HTTP remote access.
- **HTTP WAN Port:** Enter the assigned port to use for remote management.
- **Session Timeout:** Enter the session timeout period.

### CLI Management

TELNET Enable	<input checked="" type="checkbox"/>
Session Timeout	<input type="text" value="60"/>
Listen Port	<input type="text" value="23"/>
Telnet WAN Port	<input type="text" value="23"/>

- **Telnet Enable:** Select to enable telnet remote access.
- **Session Timeout:** Enter the session timeout period.
- **Listen Port:** Enter the assigned telnet listen port
- **WAN Port:** Enter the assigned port to use for remote management.

### FTPD Management

FTPD Enable	<input checked="" type="checkbox"/>
Keep old session	<input checked="" type="checkbox"/>

- **FTPD Enable:** Select to enable FTPD remote access.
- **Keep old session:** Select to enable keep old session.

### HTTPS Management

HTTPS Enable	<input type="checkbox"/>
--------------	--------------------------

- **HTTPS Enable:** Select option to enable HTTPS

### HTTPS Management

HTTP-Advanced Enable	<input type="checkbox"/>
Listen Port	<input type="text" value="0"/>

- **HTTP-Advanced Enable:** Select option to enable feature
- **Listen Port:** Enter the assigned listening port

## Configure remote access rules

*Maintenance > Access Management*

This page allows you to create and edit remote access rules. You can specify the IP address or the subnet mask of devices that are allowed or denied to remotely access your modem router and set the type of management service that they can access.

1. Log into your router management page (see “Access your router management page” on [page 22](#)).
2. Click on **Maintenance**, and click on **Access Management**.
3. Click Add to a rule and **Apply** to save settings,

#### Packet Layer

Interface	pppoe
Status	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Remote IP	
Remote IP Mask	
Service	HTTP
Rule Action	<input checked="" type="radio"/> Allow <input type="radio"/> Deny

- **Interface:** Select the interface.
- **Status:** Select whether to enable or disable remote access of the device.
- **Remote IP:** Enter the IP address of the remote device.
- **Remote IP Mask:** Enter the IP mask of the remote device.  
*Note: To allow or deny all devices to remotely access your modem router, enter “\*” on the Remote IP and Remote*
- **Service:** Select the type of remote management service that the device can or cannot access.
- **Rule Action:** Select whether to enable or disable the access rule.

#### Application Layer

User Name	admin
Interface	LAN
Match Type	Host IP/Mask
Match Condition	Equal
Host IP/Mask	
Service	GUI
Rule Action	<input checked="" type="radio"/> Allow <input type="radio"/> Deny

- **User Name:** Select the user name who can access the control rule.
- **Interface:** Select the interface.
- **Match Type:** Select the control rule type.
- **Match Condition:** Select the control rule condition.
- **Host IP/Mask:** Enter the IP address and IP mask of the remote device.
- **Service:** Select the type of remote management service that the device can or cannot access.
- **Rule Action:** Select whether to enable or disable the access rule.

### Configure the router's Ethernet port settings

*Advanced > Ethernet Settings*

This page allows you to set the link mode and enable flow control for each of the four LAN ports of your modem router.

1. Log into your router management page (see “Access your router management page” on [page 22](#)).
2. Click on **Advanced**, and click on **Ethernet Settings**.
3. Select the Interface you want to configure. Check Enable to activate interface.
4. On the **LinkMode** pull down menu select the link speed to apply and check **FlowCtrl** to enable flow control.
5. Click **Apply** to save settings.

Interface	Enable	LinkMode	FlowCtrl
LAN1	<input checked="" type="checkbox"/>	Auto	<input type="checkbox"/>
LAN2	<input checked="" type="checkbox"/>	Auto	<input type="checkbox"/>
LAN3	<input checked="" type="checkbox"/>	Auto	<input type="checkbox"/>
LAN4	<input checked="" type="checkbox"/>	Auto	<input type="checkbox"/>

### Open a device on your network to the Internet

This router can provide access to devices on your local area network to the Internet using the Virtual Server, Special Application, method (DMZ NOT recommended).

#### DMZ

*Advanced > Firewall > DMZ*

You may want to expose a specific computer or device on your network to the Internet to allow anyone to access it. Your router includes the DMZ (Demilitarized Zone) feature



that makes all the ports and services available on the WAN/Internet side of the router and forwards them to a single IP address (computer or network device) on your network. The DMZ feature is an easy way of allowing access from the Internet however, it is a very **insecure** technology and will open local area network to greater threats from Internet attacks.

It is strongly recommended to use **Virtual Server** (also called port forwarding, see “Virtual Server” on [page 35](#)) to allow access to your computers or network devices from the Internet.

1. Make sure to configure your computer or network device to use a static IP address or you can use the DHCP reservation feature (see “Set up DHCP reservation” on page 53).
2. Log into your router management page (see “Access your router management page” on [page 22](#)).
3. Click on **Advanced**, click on **Firewall**, and click on **DMZ**.
4. Select Enable next to DMZ.
5. In **DMZ Host IP Address** enter the IP address you assigned to the computer or network device to expose to the Internet.

DMZ	<input checked="" type="checkbox"/> Enable
DSL Interface	pppoe
DMZ Host IP Address	192.168.10.2

5. To save changes, click **Apply**.

**Note:** If using ADSL WAN with multiple PVCs, click the DMZ Mode drop-down list to select Multi Mode which will allow you which PVC to assign the DMZ Host.

## Virtual Server

Advanced > NAT > Virtual Server

Virtual Server (also called port forwarding) allows you to define specific ports (used or required by a specific application) and forward them to a single IP address (a computer or device) on your network. Using this feature is more secure compared to using DMZ (see “DMZ” on [page 35](#)) in which DMZ forwards all ports instead of only specific ports used by an application. An example would be forwarding a port to an network/IP camera (typically on TRENDnet IP cameras use HTTP TCP port 80 for remote access web requests) on your network for to allow remote access to it.

Since most ISPs constantly change your home IP address, to be able to access the Virtual Server port(s) from the Internet it is recommended to setup Dynamic DNS service (See DynDNS section).

1. Log into your router management page (see “Access your router management page” on [page 22](#)).
2. Click on **Advanced**, click on **NAT**, and click on **Virtual Server** option and click **Add**. To simplify configuration, there is a list of commonly used pre-defined virtual server entries to modify by clicking the drop down menu under rule name, otherwise, you can choose to manually add a new virtual server.
3. Review the virtual server settings. Click **Apply** to save settings.

Virtual Server	<input checked="" type="checkbox"/> Enable
Rule Name	<input type="text"/> << Application name
DSL Interface	pppoe
Public Port	<input type="text"/> (port or port:port)
Private Port	<input type="text"/> (port or port:port)
Protocol Type	TCP/UDP
Public IP	<input type="text"/>
Private IP	<input type="text"/>
Time Schedule	Always <input type="button" value="New Time Schedule"/>

- **Virtual Server:** Select to enable rule.
- **Rule Name:** Enter the name of the rule or select from the predefined pull down menu list.
- **DSL Interface:** The interface of the rule to be applied.
- **Public Ports:** Enter the port number required by your device from the internet. This will be the same port number used to access the device from the Internet and will include both TCP and UDP protocols.
- **Private Ports:** Enter the port number required by your device. This will be the same port number used to access the device from your network and will include both TCP and UDP protocols.

**Note:** Please refer to the device documentation to determine which ports and protocols are required.

- **Protocol Type:** Select the protocol to assign the rule.
- **Public IP:** Enter the public IP that will have access to your device (you can enter 0.0.0.0 or \* for all IP)
- **Private IP:** Enter the IP address of the device to forward the port. (e.g. 192.168.10.101).

**Note:** You should assign a static IP address to the device or use DHCP reservation to ensure the IP address of the device does not change.

- **Schedule** - Click the drop-down list assign a pre-defined schedule when the virtual server is activated or inactive.

**Note:** To define a schedule, see the "Create schedules" section.

4. To save changes, click **Apply**.

#### Example: To forward TCP port 80 to your IP camera

1. Make sure to configure your network/IP camera to use a static IP address or you can use the DHCP reservation feature (see "Set up DHCP reservation" on page 53).

**Note:** You may need to reference your camera documentation on configuring a static IP address.

1. Log into your router management page (see "Access your router management page" on page 22).
3. Click on **Advanced**, click on **NAT**, and click on **Virtual Server**.
4. In the predefine pull down list, select the entry named **WEB (80)**. In the **ID** drop-down list. Click << button.
6. Under **Private IP**, enter the IP address assigned to the camera. (e.g. 192.168.10.101)
7. Click **Apply** to save changes.

#### Port Trigger

Advanced > NAT > Port Trigger

Special applications (also called port triggering) is typically used for online gaming applications or communication applications that require a range of ports or several ports to be dynamically opened on request to a device on your network. The router will wait for a request on a specific port or range of ports (or trigger port/port range) from a device on your network and once a request is detected by your router, the router will forward a single port or multiple ports (or incoming port/port range) to the device on your network. This feature is not typically used as most devices and routers currently

use UPnP (Universal Plug and Play) to automatically configure your router to allow access for applications. See "Enable/disable UPnP on your router" on page 29.

**Note:** Please refer to the device documentation to determine if your device supports UPnP first, before configuring this feature.

1. Log into your router management page (see "Access your router management page" on page 22).
2. Click on **Advanced**, click on **NAT**, and click on **Port Trigger** option and click **Add**.
3. Review the port trigger settings and click **Apply** to save setting.

Port Trigger	<input type="checkbox"/> Enable
Rule Name	<input type="text"/>
Use Interface	pppoe ▾
Trigger Port	<input type="text"/>
Trigger Protocol	TCP/UDP ▾
Public Port	<input type="text"/>
Public Protocol	TCP/UDP ▾
Time Schedule	Always ▾ <span>New Time Schedule</span>

- **Port Trigger:** Select to enable option.
- **Rule Name:** Enter the name to assign rule.
- **Trigger:** Port or port range requested by the device. (e.g. 2000-2001 or 2000)

**Note:** Please refer to the device documentation to determine which ports are required.

- **Use Interface:** Select the interface to apply rule
- **Trigger Ports:** Port(s) forwarded to the device. (e.g. 2000-2038,2069,2081,2200-2210)
- **Trigger Protocol:** Select protocol to apply on rule
- **Public Port:** Enter the public port to assign on the rule
- **Public Protocol:** Select the public protocol to apply on rule.
- **Time Schedule:** Select the time schedule to activate rule. Select **Always** to have rule always activated or click **New Time Schedule** to create a new time schedule.

**Note:** Please refer to the device documentation to determine which ports are required.



## Prioritize traffic using QoS (Quality of Service)

*Configuration > Advanced Setting > Quality of Service*

You may want to prioritize outbound traffic for specific computers or devices on your network to have higher priority.

1. Log into your router management page (see “Access your router management page” on [page 22](#)).
2. Click on **Advanced**, and click on **Quality of Service**.
3. Review the settings and click on Apply to save settings.

### Queue Management

This page allows you to enable QoS and choose Differentiated Services Code Point (DSCP) markings to automatically mark incoming traffic without reference to a particular classifier.

Name	<input type="text"/>
Enable	<input type="checkbox"/>
Interface	<input type="text"/>
Policy	SP <input type="text"/>
Precedence	1 <input type="text"/>
Bandwidth Expression	bits <input type="text"/>
Shaping Rate	-1 <input type="text"/> -1 indicates no shaping. (bit)
Ceiling Rate	0 <input type="text"/> 0 indicates no ceiling. (bit)
Percent	0 <input type="text"/>
Burst Size	0 <input type="text"/> 0 indicates use default. (bytes)

- **Enable QoS:** Check this box to enable the QoS feature.
- **Default DSCP Mark:** Select a DSCP mark. The DSCP mark is used to classify and prioritize types of packets.
- **Interface:** Select the interface to implement this QoS queue.
- **Default Rate:** Check the Auto box to set the rate to its auto default or uncheck the box to enter the QoS rate manually.

### Queue Config

This page allows you to configure a QoS queue entry and assign it to a specific network interface. Each of the queues can be configured for a specific precedence. The queue configuration will be used in Queue Classification to place ingress packets appropriately.

Name	<input type="text"/>
Enable	<input type="checkbox"/>
Interface	<input type="text"/>
Policy	SP <input type="text"/>
Precedence	1 <input type="text"/>
Bandwidth Expression	bits <input type="text"/>
Shaping Rate	-1 <input type="text"/> -1 indicates no shaping. (bit)
Ceiling Rate	0 <input type="text"/> 0 indicates no ceiling. (bit)
Percent	0 <input type="text"/>
Burst Size	0 <input type="text"/> 0 indicates use default. (bytes)

- **Name:** Enter a QoS queue entry name.
- **Enable:** Check this box to enable this queue.
- **Interface:** Select the interface to implement this QoS queue.
- **Policy:** Select the queue policy. Options are:
  - **SP:** In Strict Priority (SP), packets with a high priority are processed first. Not until the first queue is empty will another queue be processed.
  - **WFQ:** In Weighted Fair Queuing (WFQ), each queue can be given a different priority level. Each traffic is assigned to a class and each class is given its own queue.
- **Precedence:** Select the precedence.
- **Bandwidth Expression:** Select one of the following options:
  - **Kbits:** Enter the Shaping Rate and Ceiling Rate.
  - **Percent:** Enter the Percent.
- **Burst Size:** Enter burst size.

### Queue Classification

This section allows you to configure classification rules to classify upstream traffic and assign queues which define the precedence, interface, and optionally overwrite the IP header DSCP byte. A rule consists of a class name and at least one condition. All the specified conditions in the classification rule must be satisfied for the rule to take effect.

Class Name	<input type="text"/>
Class Enable	<input type="checkbox"/>

- **Class Name:** Enter a class name.
- **Class Enable:** Check this box to enable.

### Classification Criteria

You can classify traffic based on ingress interface, Ether type, packet length, source or destination MAC address/ MAC Mask, or a combination of them. Select an option or enter the values on the fields that you want to use for the criteria. Otherwise, leave the fields empty. Depending on the selected Ether Type, the succeeding required information may vary. If packet length is used as a criteria, select the Packet Length Rule from the drop-down list and enter the Packet Length.

Assign Classification Queue	<input type="text"/>
Set VLAN Priority	<input type="text"/>
Mark DSCP	<input type="text"/>
Default VLAN ID	<input checked="" type="checkbox"/>
VLAN ID	<input type="text"/> VLAN ID (optional, range : 1 ~ 4094)
Forwarding Policy Name	<input type="text"/>

- **Assign Classification Queue:** Select the classification queue. Only enabled classification queues from the Queue Classification page are listed here.
- **Set VLAN Priority:** Select a priority.
- **Mark DSCP:** Select the DSCP mark.
- **Default VLAN ID:** Check this box to use the default VLAN ID.
- **VLAN ID:** If Default VLAN ID is not checked, enter the preferred VLAN ID.
- **Forwarding Policy Name:** Select the forwarding policy name.

## Create schedules

*Maintenance > Time Schedule*

For additional security control, your router allows you to create schedules to specify a time period when a feature on your router should be activated and deactivated. Before you use the scheduling feature on your router, ensure that your router system time is configured correctly. See [page 23](#) to configure the system time.

**Note:** You can apply a predefined schedule to the following features:

- Wireless
- Virtual Server
- Packet Filters
- QoS

Create a schedule to define the days/time period when a feature should be active or inactive:

1. Log into your router management page (see “Access your router management page” on [page 22](#)).
2. Click on **Maintenance**, and click on **Time Schedule**.
3. Review the settings and click **Add** to save settings.

Name	<input type="text"/>
Day	<input type="checkbox"/> Sun <input type="checkbox"/> Mon <input type="checkbox"/> Tue <input type="checkbox"/> Wed <input type="checkbox"/> Thu <input type="checkbox"/> Fri <input type="checkbox"/> Sat
Time	<input type="text"/> 00:00 ~ <input type="text"/> 23:59

- **Name:** Enter desired schedule name.
- **Day:** Check the day(s) to implement the schedule.
- **Time:** Specify the time period.

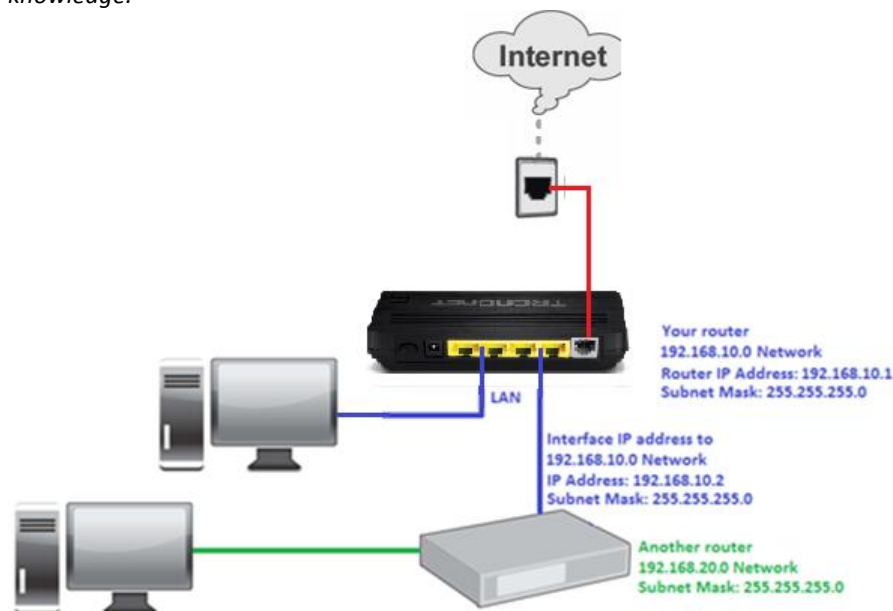
## Add static routes to your router

*Advanced > Static Route*

You may want set up your router to route computers or devices on your network to other local networks through other routers. Generally, different networks can be determined by the IP addressing assigned to those networks. Generally speaking and for the case of an example, your network may have 192.168.10.x IP addressing and

another network may have 192.168.20.x IP addressing and because the IP addressing of these two networks are different, they are separate networks. In order to communicate between the two separate networks, static routing needs to be configured. Below is an example diagram where routing is needed for devices and computers on your network to access the other network.

**Note:** Configuring this feature assumes that you have some general networking knowledge.



1. Log into your router management page (see "Access your router management page" on [page 22](#)).
2. Click on **Advanced**, and click on **Static Route**.
3. Review the settings and click Apply to save settings.

Rule Enable	Enable
Forwarding Policy Option	Enable
Rule Name	
Source IP	
Destination IP	
Gateway	
Interface Name	LAN

- **Rule Enable:** Select whether to enable or disable the rule.
- **Forwarding Policy Option:** Select whether to enable or disable routing.
- **Rule Name:** Enter desired rule name.
- **Source IP:** Enter the source IP address.
- **Source SubMask:** Enter the source subnet mask.
- **Gateway:** Enter the gateway IP address.
- **Destination IP:** Enter the destination IP address.

## Enable dynamic routing on your router

### Advanced > RIP Settings

You may want to setup your router to route computers or devices on your network to other local networks through other routers. If other routers support dynamic routing such as RIP (Routing Information Protocol), you can enable this feature on your router to automatically learn the required routes to reach those networks. It is required that the same dynamic routing protocol and version is also enabled on the other routers in order your router and the other routers to exchange information about the network.

**Note:** Configuring this feature assumes that you have some general networking knowledge.

1. Log into your router management page (see "Access your router management page" on [page 22](#)).
2. Click on **Configuration** at the top of the page, click on **Advanced**, and click on **RIP Setting**.

3. Select the Interface to configure then select appropriate dynamic routing protocol and version communicate with other routers. Click **Add** to save settings.

Interface	Receive Mode	Send Mode	Action
LAN	RIPv1	NONE	<< Add
LAN	RIPv1	NONE	

- **RIPv1:** Enables sending and receiving or exchange of routing information dynamically between your router and other routers to build routes to your network and other networks using the RIP version 1 protocol.
- **RIPv2:** Enables sending and receiving routing information dynamically between your router and other routers to build routes to your network and other networks using the RIP version 2 protocol
- **RIP 1:** Receive routing information from other routers using the RIP version 1 protocol.

## Setup Port Mapping

### Advanced > Port Mapping

Port mapping allows you to group interfaces for traffic control. Traffic is isolated from group to group. Therefore, traffic coming from an interface of a group can only be flowed to the interfaces in the same group.

By default, all interfaces belong to the Default group. You can create new groups and move interfaces to other groups. However, an interface can only be a member of one group.

1. Log into your router management page (see "Access your router management page" on [page 22](#)).
2. Click on **Advanced**, and click on **Port Mapping**.
3. Under **Port Mapping** section select **Enable**.
4. Click **New** to add a new group and select the interface from the Available Interfaces section.
5. Click the <- button to add the selected interface into the group. Or click the -> button to remove selected interface from the group.
6. Click **Apply** to save settings.

## Setup IPv6 on your router

### Advanced > IPv6

IPv6 (Internet Protocol Version 6) was developed to be the successor protocol to well known and widely used protocol IPv4 (Internet Protocol Version 4) for network addressing. The new addressing protocol is designed to minimize processing overhead by routers, significantly increase the available IP address space, provide integrated security, and open the possibility of more extensions and options. ISP have already transition their networks to accommodate IPv6 and are starting to offer IPv6 services.

**Note:** The router offers native IPv6 as well as IPv4 to IPv6 transitional connection types.

### IPv6 WAN

1. Log into your router management page (see "Access your router management page" on [page 22](#)).
2. Click on **Advanced**, and click on **IPv6 WAN**.
4. Select your IPv6 WAN type and complete the fields required by your ISP. Click Apply to save settings.

**Note:** If you are unsure which Internet connection type you are using, please contact your ISP (Internet Service Provider).

### IPv6 LAN

1. Log into your router management page (see "Access your router management page" on [page 22](#)).
2. Click on **Advanced**, and click on **IPv6 LAN**.
4. Select your **IPv6 WAN Interface** on the pull down menu and click **Apply** to save settings.

LAN IPv6 Gateway Interface Address Setting	
WAN interface	No Any IPv6 WAN Connect
LAN Link-Local Address	FE80::218:E7FF:FE5C:42E9 / 64

### Configure ADSL settings

*Advanced > ADSL*

This page allows you to select ADSL modulations, capabilities, and other options. Consult your ISP to determine the appropriate settings.

1. Log into your router management page (see "Access your router management page" on [page 22](#)).
2. Click on **Advanced**, and click on **ADSL**.
4. Select the fields required by your ISP. Click **Apply** to save settings.

ADSL modulation :	<input type="checkbox"/> G.Lite <input checked="" type="checkbox"/> G.Dmt <input checked="" type="checkbox"/> ADSL2 <input checked="" type="checkbox"/> ADSL2+ <input checked="" type="checkbox"/> ANSI(T1.413)
AnnexL Option :	<input type="checkbox"/> Enabled (Note: Only ADSL 2 supports Annex L)
AnnexM Option :	<input type="checkbox"/> Enabled (Note: Only ADSL 2/2+ support Annex M)
G.INP Option :	<input type="checkbox"/> Enable
ADSL Capability :	<input checked="" type="checkbox"/> Bitswap Enabled <input checked="" type="checkbox"/> SRA Enabled
ADSL Last Mode First :	<input type="checkbox"/> Enable

## Router Maintenance & Monitoring

### Reset your router to factory defaults

*Maintenance > Configuration Backup/Restore*

You may want to reset your router to factory defaults if you are encountering difficulties with your router and have attempted all other troubleshooting. Before you reset your router to defaults, if possible, you should backup your router configuration first, see "Backup and restore your router configuration settings" on [page 43](#).

There are two methods that can be used to reset your router to factory defaults.

- **Reset Button:** Located on the front panel of your router, see "Product Hardware Features" on [page 2](#). Use this method if you are encountering difficulties with accessing your router management page.
- OR
- **Router Management Page**

1. Log into your router management page (see "Access your router management page" on [page 22](#)).
2. Click on **Maintenance**, and click on **Configuration Backup/Restore**.
3. Under **Restore Factory Default**, click **Restore**. When prompted to confirm this action, click **OK**.

Restore Factory Default
To restore the factory default settings of the CPE, click on the "Restore" button. You will be asked to confirm your decision.
<div>Restore ...</div>

## Router Default Settings

<b>Administrator User Name</b>	admin
<b>Administrator Password</b>	admin
<b>Router IP Address</b>	192.168.10.1
<b>Router Subnet Mask</b>	255.255.255.0
<b>DHCP Server IP Range</b>	192.168.10.101-192.168.199
<b>Wireless</b>	Enabled
<b>SSID (wireless network name)</b>	Please refer sticker or device label
<b>Wireless Security</b>	Please refer sticker or device label
<b>802.11 Mode</b>	2.4GHz 802.11b/g/n mixed mode
<b>Channel</b>	Auto Channel

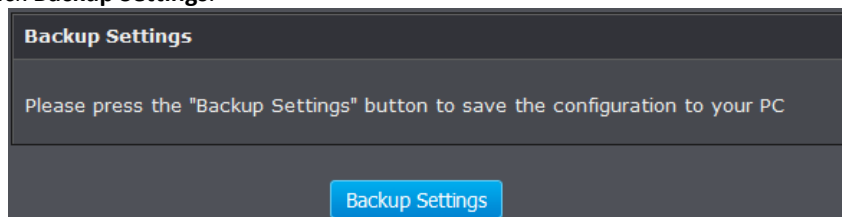
## Backup and restore your router configuration settings

### *Maintenance > Configuration Backup/Restore*

You may have added many customized settings to your router and in the case that you need to reset your router to default, all your customized settings would be lost and would require you to manually reconfigure all of your router settings instead of simply restoring from a backed up router configuration file.

#### To backup your router configuration:

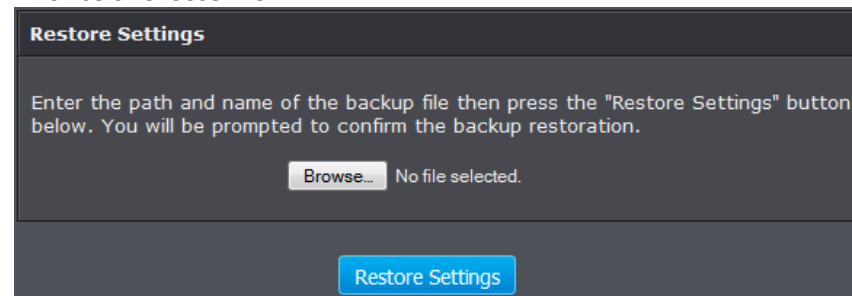
1. Log into your router management page (see "Access your router management page" on [page 22](#)).
2. Click on **Maintenance**, and click on **Configuration Backup/Restore**.
3. Click **Backup Settings**.



3. Depending on your web browser settings, you may be prompted to save a file (specify the location) or the file may be downloaded automatically to the web browser settings default download folder. (Default Filename: *config.bin*)
4. Save the configuration file to location on your computer.

#### To restore your router configuration:

1. Log into your router management page (see "Access your router management page" on [page 22](#)).
2. Click on **Maintenance**, and click on **Configuration Backup/Restore**.
3. Under **Restore Settings**, next to **Load Settings**, depending on your web browser, click on **Browse** or **Choose File**.



A separate file navigation window should open.

4. Navigate to the location of the router configuration file to restore.  
(Default Filename: *config.bin*).
5. Select the router configuration file to restore and click **Restore Settings**.  
(Default Filename: *config.bin*). If prompted, click **Yes** or **OK**.
6. Wait for the router to restore settings.



## Upgrade your router firmware

### Maintenance > FW Upgrade

TRENDnet may periodically release firmware upgrades that may add features or fix problems associated with your TRENDnet router model and version. To check if there is a firmware upgrade available for your device, please check your TRENDnet model and version using the link. <http://www.trendnet.com/downloads/>

In addition, it is also important to verify if the latest firmware version is newer than the one your router is currently running. To identify the firmware that is currently loaded on your router, log in to the router, and check the version located at the top right of the router management page. If there is a newer version available, also review the release notes to check if there were any new features you may want or if any problems were fixed that you may have been experiencing.

1. If a firmware upgrade is available, download the firmware to your computer.
2. Unzip the file to a folder on your computer.

#### Please note the following:

- Do not interrupt the firmware upgrade process. Do not turn off the device or press the Reset button during the upgrade.
- If you are upgrade the firmware using a laptop computer, ensure that the laptop is connected to a power source or ensure that the battery is fully charged.
- Disable sleep mode on your computer as this may interrupt the firmware upgrade process.
- Do not upgrade the firmware using a wireless connection, only using a wired network connection.
- Any interruptions during the firmware upgrade process may permanently damage your router.

1. Log into your router management page (see "Access your router management page" on [page 22](#)).

**Note:** You can check your router's current firmware version at the top right of the page.

2. Click on **Maintenance**, and click on **FW Upgrade**.

**Note:** This page also displays the current firmware version of your router.

3. Depending on your web browser, next to **Upgrade Firmware**, click **Browse** or **Choose File**.

Upgrade Firmware	
Current Firmware Version	V1.00.B12
Upgrade Firmware	<input type="button" value="Browse..."/> No file selected.
<input type="button" value="Apply"/>	

4. Navigate to the folder on your computer where the unzipped firmware file (.bin) is located and select it.
5. Click **Upgrade** to start the firmware upgrade process. If prompted, click **yes** or **OK**.

## Restart your router

*Maintenance > Reboot Device*

You may want to restart your router if you are encountering difficulties with your router and have attempted all other troubleshooting.

There are two methods that can be used to restart your router.

- **Turn the router off** disconnect the power adapter from the rear panel of your router for 10 seconds and reconnect the power adapter, see "Product Hardware Features" on [page 2](#).  
Use this method if you are encountering difficulties with accessing your router management page. This is also known as a hard reboot or power cycle.  
OR
- **Router Management Page:** This is also known as a soft reboot or restart.

1. Log into your router management page (see "Access your router management page" on [page 22](#)).
2. Click on **Maintenance**, and click on **Reboot Device**. If prompted, click **yes** or **OK**.
3. Click **Reboot** to restart the router. If prompted, click **yes** or **OK**.

In the event that the device stops responding correctly or in some way stops functioning, you can perform a reboot. Your settings will not be changed. To perform the reboot, click on the "reboot" button below. You will be asked to confirm your decision. The reboot will be complete when the system light starts blinking.

Reboot

## Check connectivity using the router management page

*Maintenance > Ping*

For troubleshooting purposes, you may want to check your router connectivity using the ping (also known as a network connectivity test) test tool on your router management page.

1. Log into your router management page (see "Access your router management page" on [page 22](#)).
2. Click on **Maintenance**, and click on **Ping**.
3. Next to **Host IPv4 Address**, enter in the IP address (e.g. *192.168.10.101*) or host name (e.g. *www.trendnet.com*) to test and click **Ping**.

### Ping Test

Host IPv4 Address:

Ping

Stop

4. You will receive a *success* or *fail* result message of the address you entered providing a basic indicating of the router's connectivity to the Internet or devices that are connected to your network.

### Ping Result

```
PING 192.168.10.1 (192.168.10.1): 56 data bytes
64 bytes from 192.168.10.1: seq=0 ttl=64 time=30.000 ms
64 bytes from 192.168.10.1: seq=1 ttl=64 time=0.000 ms
64 bytes from 192.168.10.1: seq=2 ttl=64 time=0.000 ms
```

## Manage Initialization Scripts

*Maintenance > Init Script*

This page allows you to show, delete, and import initialization scripts running on customer-premises equipment (CPE), such as telephones, routers, or set-top boxes, during system startup or shutdown.

Init start scripts are scripts that run before the system starts up. Init end scripts are scripts that run before the system shuts down.

1. Log into your router management page (see "Access your router management page" on [page 22](#)).
2. Click on **Maintenance**, and click on **Init script**.
3. Click **Browse** and select your script.
4. Click **Import Script** to import script to router.

### Init Start Script

Press 'Import Script' button to import init start script.Press the 'Show Start Script' button to show the Init Start Script on your PC.To delete the Init Start Script of the CPE, click on the "Delete" button.You will be asked to confirm your decision.

Script On Start
 No file selected.

### Init End Script

Press 'Import Script' button to import init end script.Press the 'Show End Script' button to show the Init End Script on your PC.To delete the Init End Script of the CPE, click on the "Delete" button.You will be asked to confirm your decision.

Script On End
 No file selected.

5. To show scripts on your computer click **Show script**. Press **Delete** to remove script.

## Check Internet connectivity using the router management page

### *Maintenance > Diagnostic*

This page allows you to test the connectivity of the physical and protocol layers on the WAN side.

1. Log into your router management page (see "Access your router management page" on [page 22](#)).
2. Click on **Maintenance**, and click on **Diagnostic**.
3. Select your DSL interface and click **test**.

ATM F4/F5 Loopback Diagnostics		
DSL Interface	PVC:0/35	<input type="button" value="test"/>
ATM F4 SENGMENT	Repetitions Count	1
	Response Timeout	1 ms
	Success Response Count	0
	Failure Response Count	0
	Average Response Time	0 ms
	Minimum Response Time	0 ms
	Maximum Response Time	0 ms
	Test result	
	Repetitions Count	1
	Response Timeout	1 ms

## Check the router system information

### *Status > Summary*

You may want to check the system information of your router such as WAN (Internet) connectivity, wireless and wired network settings, and router MAC address information.

1. Log into your router management page (see "Access your router management page" on [page 22](#)).
2. Click on **Status**.
3. Review the device information.

## System

System	
New FirmWare	Without new firmware now
Firmware Version	V1.00.B12
Modem Type	ADSL2+ Router
Modem Vendor	TRENDNET
Modem OUI	0018E7
Modem Serial Number	0018E75C42E9
Uptime	21 hour 37 min 59 sec
Current Time	2014/09/13 13:47:53

- **Firmware Version:** Displays the firmware version currently loaded on the router
- **Modem Type:** Displays the modem type
- **Modem Vendor:** Displays modem vendor
- **Modem OUI:** Displays modem OUI
- **Modem Serial Number:** Serial number of modem
- **Uptime:** Time duration of modem up time
- **Current Time:** Time of router

## DSL Link Status

DSL Link Status		
Modulation Type		
	Downstream	Upstream
Current Rate(Kbps)	0	0

- **Modulation Type:** Display the modulation applied on the router
- **Current Rate:** Downstream and upstream data rate

## ATM PVC Status

ATM PVC Status	
VPI	0
VCI	35
Link Type	EoA
Encapsulation	LLC

- **VPI:** Current VPI settings applied on the router
- **VCI:** Current VCI settings applied on the router
- **Link Type:** Link type applied on the router
- **Encapsulation:** Current encapsulation applied on the router.

## ATM PVC Status

Internet Connection Status	
Interface	PVC:0/35
Connection Status	Not Connected

- **Interface:** Current router PVC interface
- **Connection Status:** Current internet connection status

## LAN Status

LAN Status	
IP Address	192.168.10.1
Subnet Mask	255.255.255.0
MAC Address	00:18:E7:5C:42:E9
DHCP Server	Enabled

- **IP Address:** Router's IP address
- **Subnet Mask:** Router's subnet mask
- **MAC Address:** MAC address of router
- **DHCP Server:** Current status of router's DHCP

**Wireless Interface**

Wireless Port			
Mode	802.11n + 802.11g + 802.11b		
Channel	6		
SSID	Enable	MAC Address	Security Mode
media72	Yes	00:18:E7:5C:42:E9	WPA2-AES-PSK
TRENDnet722_2.4GHz_Guest	Yes	00:18:E7:5C:42:EA	None

- **Mode:** Current wireless mode
- **Channel:** Wireless channel
- **SSID:** Wireless network name
- **MAC Address:** Wireless MAC address
- **Security Mode:** Wireless encryption of security

**Check the router IPv6 status**

*Status > IPv6 Info*

You may want to check the system IPv6 information of your router.

1. Log into your router management page (see “Access your router management page” on [page 22](#)).
2. Click on **Status** and **IPv6 Info**.
3. Review the device information.

LAN Status	
LAN Link-Local Address:	fe80::218:e7ff:fe5c:42e9

**Check the router IPv6 status**

*Status > ADSL Info*

You may want to check the system ADSL information of your router.

1. Log into your router management page (see “Access your router management page” on [page 22](#)).
2. Click on **Status** and **ADSL Info**.
3. Review the device information.

Rules		
Status	EstablishingLink	
Total Time	22 hour 2 min 29 sec	
Modulation Type		
Standard Used		
Standards Supported		
Link Encapsulation Used	G.992.3_Annex_K_ATM,	
Link Encapsulation Supported		
Link Encapsulation Requested		
Line Encoding	DMT	
Data Path	L2	
Interleave Depth		
ATUR Vendor	5245544b	
ATUR Country	181	
ATUC Vendor	ffffff	
ATUC Country	255	
	Downstream	Upstream
Current Rate(Kbps)	0	0
Noise Margin(dB)	0	0
Attenuation(dB)	0	0
Output Power(dBm)	0	0

**Check the router Wireless clients**

*Status > Wireless Clients*

This page displays all connected wireless clients.

1. Log into your router management page (see “Access your router management page” on [page 22](#)).
2. Click on **Status** and **Wireless Clients**.
3. Review the device information.

SSID	IP Address	MAC Address	RSSI
------	------------	-------------	------

## Check the router LAN clients

Status > LAN Clients

This page displays all connected clients.

1. Log into your router management page (see "Access your router management page" on [page 22](#)).
2. Click on **Status** and **LAN Clients**.
3. Review the device information.

Host Name	IP Address	MAC Address	Address Source	Lease Time
TV-IP343PI	192.168.10.107	00:0F:0D:26:40:6E	DHCP	66777
TRENDnetACER-PC	192.168.10.101	00:26:2D:5B:46:53	DHCP	86400
TV-IP302PI	192.168.10.101	00:14:D1:95:00:2D	DHCP	0
tew-820ap	192.168.10.103	D8:FE:E3:3E:B0:4D	DHCP	0
TV-IP342PI	192.168.10.105	00:0F:0D:26:9A:3E	DHCP	0
unknow	192.168.10.118	1C:75:08:A4:E0:4A	Static	0
Apple-TV	192.168.10.104	B8:17:C2:B3:B8:91	DHCP	64432
unknow	192.168.10.109	D8:EB:97:CD:4A:E8	DHCP	81439

## Check the router Routing Table

Status > Routing Table

This page displays all connected clients.

1. Log into your router management page (see "Access your router management page" on [page 22](#)).
2. Click on **Status** and **Routing Table**.
3. Review the device information.

Destination	Gateway	GenMask	Flags	Interface
192.168.10.0	0.0.0.0	255.255.255.0	U	br0

## Check the router Basic Statistics

Status > Statistics > Basic Statistics

This page displays all connected clients.

1. Log into your router management page (see "Access your router management page" on [page 22](#)).

2. Click on **Status** and **Basic Statistics**.

3. Review the device information.

Internet Connections				
LAN Device				
Tx OK	110828	Packets		
Rx OK	88531	Packets		
Tx Error	0	Packets		
Rx Error	0	Packets		
Wireless Port				
Tx OK	13608	Packets		
Rx OK	1477315	Packets		
Tx Error	36	Packets		
Rx Error	0	Packets		
LAN Ports				
	LAN1	LAN2	LAN3	LAN4
Link Status	up	up	up	Auto
Tx OK(Packets)	0	110441	0	0
Rx OK(Packets)	0	88379	0	0
Rx Drop (Packets)	0	0	0	0
Rx Error(Packets)	0	0	0	0

## Check the router DSL Statistics

Status > Statistics > DSL Statistics

This page displays all connected clients.

1. Log into your router management page (see "Access your router management page" on [page 22](#)).
2. Click on **Status** and **DSL Statistics**.
3. Review the device information.

- **IP Address:** Router's IP address
- **Subnet Mask:** Router's subnet mask
- **MAC Address:** MAC address of router

	DownstreamDownstream	Downstream
Trellis		
SNR Margin (dB)	0.0	0.0
Attenuation (dB)	0.0	0.0
Output Power(dBm)	0.0	0.0
Attainable Rate (Kbps)	0	0
G.INP		
Rate (Kbps)	0	0
K (number of bytes in DMT frame)	0	0
R (number of check bytes in RS code word)	0	0
N (RS codeword size)		
L (number of bits in DMT frame)		
S (RS code word size in DMT frame)		

## View your router log

Status > Logs

Your router log can be used to obtain activity information on the functionality of your router or for troubleshooting purposes.

1. Log into your router management page (see "Access your router management page" on [page 22](#)).
2. Click on **Maintenance**, and click on **Syslog**.
3. Review the device log information. You can filter the log view by selecting a particular **Facility**, **Severity**, **Module**, or **History** option.

Facility	Severity	Module	History	
all	debug	all	No	
<div><div>&lt;&lt;</div><div>&gt;&gt;</div><div>&gt; </div><div>Clear</div><div>Clear history</div><div>Backup logs</div></div>				
Page 1 Of 14				
Time	Fac.	Fac.	Module	Message
2014-09-13 12:19:28	user	info	system	Renewal subscription: total_subscription [1]
2014-09-13 12:19:28	user	info	system	HTTP REQUEST : SUBSCRIBE /upnp/event/WFAWLANConfig1 (HTTP/1.1)
2014-09-13 12:17:31	user	info	system	Renewal subscription: total_subscription [1]
2014-09-13 12:17:31	user	info	system	HTTP REQUEST : SUBSCRIBE /upnp/event/WFAWLANConfig1 (HTTP/1.1)
2014-09-13 12:15:34	user	info	system	Renewal subscription: total_subscription [1]

- **First Page:** Displays the first page of the log.
- **Last Page:** Displays the last page of the log.
- **Previous Page:** Display the log page previous to the current. The **Page: 1/1** will display the current page.
- **Next Page:** Displays the log page next to the current.
- **Clear Log:-** Clears log entries
- **Clear History:** Clear all log entries
- **Refresh:** The **Page: 1/1** will display the current page.
- **Backup Logs:** Click to save logs to a local text file on your local hard drive.

## View your router traffic

Status > Traffic Meter

Your router log can be used to obtain activity information on the functionality of your router or for troubleshooting purposes.

1. Log into your router management page (see "Access your router management page" on [page 22](#)).
2. Click on **Status**, and click on **Traffic Meter**.
3. On the **Traffic Data Interface** section, check the **Status** box of the interface to view its traffic. You may check more than one interface.



4. On the **Traffic Bandwidth Interval** section, enter the interval of refreshing the traffic bandwidth.

Interface	Status
LANIP1:192.168.10.1	<input checked="" type="checkbox"/> Enable
PVC0:0/35	<input type="checkbox"/> Enable

Traffic Bandwidth Interval	
Interval	10 (1~10000 seconds)

## Configure your router log

Maintenance > Syslog

You may want send your router log to your e-mail address or to an external log server (also known as Syslog server) so you can check it periodically while away from home. You may also want to only see specific categories of logging.

### Send router logs to an external log server

Maintenance > Syslog

1. Log into your router management page (see "Access your router management page" on [page 22](#)).
2. Click on **Maintenance**, click on **Syslog**.
3. Next to **Syslog** and check **Enable**.

Log Generate Enable Options	
SysLog	<input checked="" type="checkbox"/> Enable
Kernel Common Message	<input type="checkbox"/> Enable

4. Click **Add** in **Log Rules Settings**. Click **Apply** to save settings.

Module	all
Facility	all
Severity	debug
Location	<input checked="" type="radio"/> Remote Server <input type="radio"/> Mail
Syslog Server IP	

- **Module:** Select the module type.
- **Facility:** Select the facility type.
- **Severity:** Select the severity level.  
Note: **emerg** is the highest level while debug is the lowest level.
- **Location:** Enter an assigned location for your log.  
**Note:** The succeeding fields may vary depending

If the Location is set to Mail, configure the following settings:

SMTP Server IP of Domain Name	
Source E-mail Address	
Destination E-mail Address	
SMTP Authentication	<input type="checkbox"/> Enable
SMTP Username	
SMTP Password	
Confirm Password	

- **SMTP Server IP of Domain Name:** Enter the IP address (i.e. 10.10.10.10) or domain name (i.e. mail.trendnet.com) of your e-mail server.
- **Source E-mail Address:** Enter the sender or source mail address. You can use this to easily identify the notification in your email inbox. (i.e. modem\_router@trendnet.com)
- **Destination E-mail Address:** Enter your e-mail address.
- **SMTP Authentication:** Check the box if your e-mail server requires authentication. If enabled, enter the account name and password in the
- **SMTP Username:** Enter the account name required for authentication by your SMTP mail server.

- **SMTP Password/Confirm Password:** Enter the password required for authentication by your SMTP mail server. Enter the password again in the

### Send router logs to your e-mail address

*Maintenance > Syslog*

1. Log into your router management page (see “Access your router management page” on [page 22](#)).
2. Click on **Maintenance**, click on **Syslog**.
3. Review the e-mail log settings and click **Apply** to save setting.

E-mail Log Periodically	
SMTP Server	<input type="checkbox"/> Enable
SMTP Server IP	<input type="text"/>
Source E-mail Address	<input type="text"/>
Destination E-mail Address	<input type="text"/>
SMTP Authentication	<input type="checkbox"/> Enable
SMTP Username	<input type="text"/>
SMTP Password	<input type="password"/>
Confirm Password	<input type="password"/>
Time Frequency	<input type="text" value="1"/> (hours)

- **SMTP Server:** Check the box to enable the email log notification.
- **SMTP Server IP:** Enter the IP address (i.e. 10.10.10.10) or domain name (i.e. mail.trendnet.com) of your e-mail server.
- **Source E-mail Address:** Enter the sender or source mail address. You can use this to easily identify the notification in your email inbox. (i.e. modem\_router@trendnet.com)
- **Destination E-mail Address:** Enter your e-mail address.
- **SMTP Authentication:** Check the box if your e-mail server requires authentication.
- **SMTP Username:** Enter the account name required for authentication by your
- **SMTP Password/Confirm Password:** Enter the password required for authentication by your SMTP mail server. Enter the password again in the
- **Time Frequency:** Select the frequency of logging e-mails.

## Enable SNMP on your router

*Advanced > SNMP*

SNMP (Simple Network Management Protocol) is a network management protocol used to monitor (read) and/or manage (write) multiple network devices on a network. This preconfigured external SNMP server.

1. Log into your router management page (see “Access your router management page” on [page 22](#)).
2. Click on **Advanced** and click on **SNMP**.
3. Review the options for SNMP and click **Apply** to save settings..

SNMP	<input type="checkbox"/> Enable
System Contact	<input type="text"/>
System Name	<input type="text"/>
System Location	<input type="text"/>
Public community	<input type="text"/>
Private community	<input type="text"/>
Trap	<input type="checkbox"/> Enable
Trap Version	<input type="text" value="SNMPv1"/>
Trap Address	<input type="text"/>

- **System Contact:** Enter the contact person or contact information for your modem router.
- **System Name:** Enter an assigned name for your modem router.
- **System Location:** Enter an assigned location for your modem router.
- **Public Community/Private Community:** Enter a public and private community name.
- **Trap:** Check this box to enable the Trap function, then provide the following information:
- **Trap Version:** Select an SNMP trap version.
- **Trap Address:** Enter the destination IP address of the SNMP trap.

## Enable TR-069 on your router

*Maintenance > TR069 Setting*

TR-069 is a network management protocol used to remote manage multiple network devices on a network typically by ISPs (Internet Service Providers). TR069 usually used in conjunction with ACS (Auto Configuration Servers) server managed by your ISP.

1. Log into your router management page (see "Access your router management page" on [page 22](#)).
2. Click on **Maintenance** and click on **TR069 Setting**.
3. Please consult your ISP for the required TR069 settings for remote management. Click **Apply** to save settings.

TR069 settings	
Enable	<input checked="" type="checkbox"/>
ACS URL Address	<input type="text"/>
ACS User Name	<input type="text"/>
ACS Password	<input type="password"/>
Confirm Password	<input type="password"/>
Connection Request Enable	<input checked="" type="checkbox"/>
Connection Request Port	<input type="text" value="7547"/>
Connection Request User Name	<input type="text"/>
Connection Request Password	<input type="password"/>
Confirm Password	<input type="password"/>
Verify Server Certificate	<input checked="" type="checkbox"/>
Use Soap v1.2	<input type="checkbox"/>
Periodic Inform	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Periodic Inform Interval	<input type="text" value="0"/> seconds

- **Enable:** Check this box to enable TR069.
- **ACS URL Address:** Enter the URL of the Auto-Configuration Server (ACS).

- **ACS User Name:** Enter the user name of your modem router when connecting to the ACS.
- **ACS Password/Confirm Password:** Enter the password that your modem router should use when connecting to the ACS. Re-enter the password on the Confirm
- **Connection Request Enable:** Check the box to enable the connection request.
- **Connection Request Port:** Enter the port that issues the request.
- **Connection Request User Name:** Enter the connection request user name.
- **Connection Request Password/Confirm Password:** Enter the connection request password. Re-enter the password on the Confirm Password field.
- **Verify Server Certificate:** Check this box to verify server certificates.
- **Use Soap v1.2:** Check this box to enable the SOAP protocol.
- **Periodic Inform:** Select Enable to let your modem router to send remote procedure calls (RPC) to the ACS server at system startup and will continue sending RPCs periodically. When disabled, your modem router will send RPCs to the ACS server at system startup only.
- **Periodic Inform Interval:** Enter the interval time of sending RPCs.

## Troubleshooting

**Q: I typed `http://192.168.10.1` in my Internet Browser Address Bar, but an error message says “The page cannot be displayed.” How can I access the router management page?**

**Answer:**

1. Check your hardware settings again. See “Router Installation” on [page 2](#).
2. Make sure the LAN and WLAN lights are lit.
3. Make sure your network adapter TCP/IP settings are set to [Obtain an IP address automatically](#) or [DHCP](#) (see the steps below).
4. Make sure your computer is connected to one of the router's LAN ports
5. Press on the factory reset button for 15 seconds, the release.

### Windows 7

- a. Go into the **Control Panel**, click **Network and Sharing Center**.
- b. Click **Change Adapter Settings**, right-click the **Local Area Connection** icon.
- c. Then click **Properties** and click **Internet Protocol Version 4 (TCP/IPv4)**.
- d. Then click **Obtain an IP address automatically** and click **OK**.

### Windows Vista

- a. Go into the **Control Panel**, click **Network and Internet**.
- b. Click **Manage Network Connections**, right-click the **Local Area Connection** icon and click **Properties**.
- c. Click **Internet Protocol Version (TCP/IPv4)** and then click **Properties**.
- d. Then click **Obtain an IP address automatically** and click **OK**.

### Windows XP/2000

- a. Go into the **Control Panel**, double-click the **Network Connections** icon
- b. Right-click the **Local Area Connection** icon and the click **Properties**.
- c. Click **Internet Protocol (TCP/IP)** and click **Properties**.
- d. Then click **Obtain an IP address automatically** and click **OK**.

**Note:** If you are experiencing difficulties, please contact your computer or operating system manufacturer for assistance.

**Q: I am not sure what type of Internet Account Type I have for my Cable/DSL connection. How do I find out?**

**Answer:**

Contact your Internet Service Provider (ISP) for the correct information.

**Q: The Wizard does not appear when I access the router. What should I do?**

**Answer:**

1. Click on Setup Wizard on the left hand side.
2. Near the top of the browser, “Pop-up blocked” message may appear. Right click on the message and select Always Allow Pop-ups from This Site.
3. Disable your browser's pop up blocker.

**Q: I went through the Wizard, but I cannot get onto the Internet. What should I do?**

**Answer:**

1. Verify that you can get onto the Internet with a direct connection into your ADSL modem from your ISP (meaning, plug your computer directly to the modem and verify that your single computer (without the help of the router) can access the Internet).
2. Power cycle your modem router. Unplug the power to the modem router. Wait 30 seconds, and then reconnect the power to the modem router. Wait for the modem router to fully boot up, then try to re-access the Internet .
3. Contact your ISP and verify all the information that you have in regards to your Internet connection settings is correct.

**Q: I cannot connect wirelessly to the router. What should I do?**

**Answer:**

1. Double check that the WLAN light on the router is lit.
2. Power cycle the router. Unplug the power to the router. Wait 15 seconds, then plug the power back in to the router.
3. Contact the manufacturer of your wireless network adapter and make sure the wireless network adapter is configured with the proper SSID. The preset SSID is TRENDnet(model\_number).
4. To verify whether or not wireless is enabled, login to the router management page, click on *Wireless*.
5. Please see “Steps to improve wireless connectivity” on [page 19](#) if you continue to have wireless connectivity problems.

## Appendix

### How to find your IP address?

**Note:** Please note that although the following procedures provided to follow for your operating system on configuring your network settings can be used as general guidelines, however, it is strongly recommended that you consult your computer or operating system manufacturer directly for assistance on the proper procedure for configuring network settings.

#### Command Prompt Method

##### **Windows 2000/XP/Vista/7**

1. On your keyboard, press **Windows Logo+R** keys simultaneously to bring up the Run dialog box.
2. In the dialog box, type **cmd** to bring up the command prompt.
3. In the command prompt, type **ipconfig /all** to display your IP address settings.

##### **MAC OS X**

1. Navigate to your **Applications** folder and open **Utilities**.
2. Double-click on **Terminal** to launch the command prompt.
3. In the command prompt, type **ipconfiggetifaddr<en0 or en1>** to display the wired or wireless IP address settings.

**Note:** **en0** is typically the wired Network and **en1** is typically the wireless Airport interface.

#### Graphical Method

##### **MAC OS 10.6/10.5**

1. From the Apple menu, select **System Preferences**.
2. In System Preferences, from the **View** menu, select **Network**.
3. In the Network preference window, click a network port (e.g., Network, AirPort, modem). If you are connected, you'll see your IP address settings under "Status:"

##### **MAC OS 10.4**

1. From the Apple menu, select **Location**, and then **Network Preferences**.
2. In the Network Preference window, next to "Show:", select **Network Status**. You'll see your network status and your IP address settings displayed.

**Note:** If you are experiencing difficulties, please contact your computer or operating system manufacturer for assistance.

### How to configure your network settings to obtain an IP address automatically or use DHCP?

**Note:** Please note that although the following procedures provided to follow for your operating system on configuring your network settings can be used as general guidelines, however, it is strongly recommended that you consult your computer or operating system manufacturer directly for assistance on the proper procedure for configuring network settings.

#### **Windows 7**

- a. Go into the **Control Panel**, click **Network and Sharing Center**.
- b. Click **Change Adapter Settings**, right-click the **Local Area Connection** icon.
- c. Then click **Properties** and click **Internet Protocol Version 4 (TCP/IPv4)**.
- d. Then click **Obtain an IP address automatically** and click **OK**.

#### **Windows Vista**

- a. Go into the **Control Panel**, click **Network and Internet**.
- b. Click **Manage Network Connections**, right-click the **Local Area Connection** icon and click **Properties**.
- c. Click **Internet Protocol Version (TCP/IPv4)** and then click **Properties**.
- d. Then click **Obtain an IP address automatically** and click **OK**.

#### **Windows XP/2000**

- a. Go into the **Control Panel**, double-click the **Network Connections** icon
- b. Right-click the **Local Area Connection** icon and the click **Properties**.
- c. Click **Internet Protocol (TCP/IP)** and click **Properties**.
- d. Then click **Obtain an IP address automatically** and click **OK**.

#### **MAC OS 10.4/10.5/10.6**

- a. From the **Apple**, drop-down list, select **System Preferences**.
- b. Click the **Network** icon.
- c. From the **Location** drop-down list, select **Automatic**.
- d. Select and view your Network connection.
  - In MAC OS 10.4, from the **Show** drop-down list, select **Built-in Network** and select the **TCP/IP** tab.
  - In MAC OS 10.5/10.6, in the left column, select **Network**.
- e. Configure TCP/IP to use DHCP.
  - In MAC 10.4, from the **Configure IPv4**, drop-down list, select **Using DHCP** and click the **Apply Now** button.
  - In MAC 10.5, from the **Configure** drop-down list, select **Using DHCP** and click the **Apply** button.

In MAC 10.6, from the **Configure** drop-down list, select **Using DHCP** and click the **Apply** button.

f. Restart your computer.

**Note:** If you are experiencing difficulties, please contact your computer or operating system manufacturer for assistance.

#### How to find your MAC address?

In Windows 2000/XP/Vista/7,

Your computer MAC addresses are also displayed in this window, however, you can type **getmac -v** to display the MAC addresses only.

In MAC OS 10.4,

1. **Apple Menu > System Preferences > Network**
2. From the **Show** menu, select **Built-in Network**.
3. On the **Network** tab, the **Network ID** is your MAC Address.



In MAC OS 10.5/10.6,

1. **Apple Menu > System Preferences > Network**
2. Select **Network** from the list on the left.
3. Click the **Advanced** button.
3. On the **Network** tab, the **Network ID** is your MAC Address.


#### How to connect to a wireless network using the built-in Windows utility?

**Note:** Please note that although the following procedures provided to follow for your operating system on configuring your network settings can be used as general guidelines, however, it is strongly recommended that you consult your computer or operating system manufacturer directly for assistance on the proper procedure for connecting to a wireless network using the built-in utility.

##### Windows 7

1. Open Connect to a Network by clicking the network icon ( or ) in the notification area.
2. In the list of available wireless networks, click the wireless network you would like to connect to, then click **Connect**.
4. You may be prompted to enter a security key in order to connect to the network.
5. Enter in the security key corresponding to the wireless network, and click **OK**.

##### Windows Vista

1. Open Connect to a Network by clicking the **Start Button**  and then click **Connect To**.
2. In the **Show** list, click **Wireless**.
3. In the list of available wireless networks, click the wireless network you would like to connect to, then click **Connect**.
4. You may be prompted to enter a security key in order to connect to the network.
5. Enter in the security key corresponding to the wireless network, and click **OK**.

##### Windows XP

1. Right-click the network icon in the notification area, then click **View Available Wireless Networks**.
2. In **Connect to a Network**, under **Available Networks**, click the wireless network you would like to connect to.
3. You may be prompted to enter a security key in order to connect to the network.
4. Enter in the security key corresponding to the wireless network, and click **Connect**.



**Federal Communication Commission Interference Statement**

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules.

These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

**FCC Caution:** Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

**IMPORTANT NOTE:****FCC Radiation Exposure Statement:**

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance

20cm between the radiator & your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Country Code selection feature to be disabled for products marketed to the US/CANADA.

**RoHS**

This product is RoHS compliant.

**Europe – EU Declaration of Conformity**

This device complies with the essential requirements of the R&TTE Directive 1999/5/EC, 2006/95/EC and 2009/125/EC.

**Regulation (EC) No. 1275/2008**

**Regulation (EC) No. 278/2009**

**EN60950-1 : 2006 + A11 : 2009 + A1: 2010 + A12: 2011**

Safety of Information Technology Equipment

**EN 50385 : 2002**

Product standard to demonstrate the compliance of radio base stations and fixed terminal stations for wireless telecommunication systems with the basic restrictions or the reference levels related to human exposure to radio frequency electromagnetic fields

(110MHz - 40 GHz) - General public

**EN 300 328 V1.7.1 : (2006-10) Class B**

Electromagnetic compatibility and Radio spectrum Matters (ERM); Wideband Transmission systems; Data transmission equipment operating in the 2,4 GHz ISM band and using spread spectrum modulation techniques; Harmonized EN covering essential requirements under article 3.2 of the R&TTE Directive

**EN 301 489-1 V1.9.2 : (2011-09)**

Electromagnetic compatibility and Radio Spectrum Matters (ERM); ElectroMagnetic Compatibility (EMC) standard for radio equipment and services; Part 1: Common technical requirements

**EN 301 489-17 V2.1.1 : (2009-05)**

Electromagnetic compatibility and Radio spectrum Matters (ERM); ElectroMagnetic Compatibility (EMC) standard for radio equipment; Part 17: Specific conditions for 2,4 GHz wideband transmission systems, 5 GHz high performance RLAN equipment and 5,8 GHz Broadband Data Transmitting Systems

In Italy the end-user should apply for a license at the national spectrum authorities in order to obtain authorization to use the device for setting up outdoor radio links and/or for supplying public access to telecommunications and/or network services.

This device may not be used for setting up outdoor radio links in France and in some areas the RF output power may be limited to 10 mW EIRP in the frequency range of 2454 – 2483.5 MHz. For detailed information the end-user should contact the national spectrum authority in France.





<b>[cs]</b> Český [Czech]	TRENDnet tímto prohlašuje, že tento TEW-721BRM je ve shodě se základními požadavky a dalšími příslušnými ustanoveními směrnice 1999/5/ES, 2006/95/ES, a 2009/125/ES.
<b>[da]</b> Dansk [Danish]	Undertegnede TRENDnet erklærer herved, at følgende udstyr TEW-721BRM overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF, 2006/95/EF, og 2009/125/EF.
<b>[de]</b> Deutsch [German]	Hiermit erklärt TRENDnet, dass sich das Gerät TEW-721BRM in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EG, 2006/95/EG und 2009/125/EG befindet.
<b>[et]</b> Eesti [Estonian]	Käesolevaga kinnitab TRENDnet seadme TEW-721BRM vastavust direktiivi 1999/5/EÜ, 2006/95/EÜ ja 2009/125/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
<b>[en]</b> English	Hereby, TRENDnet, declares that this TEW-721BRM is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC, 2006/95/EC, and 2009/125/EC.
<b>[es]</b> Español [Spanish]	Por medio de la presente TRENDnet declara que el TEW-721BRM cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE, 2006/95/CE, 2009/125/CE y.
<b>[el]</b> Ελληνική [Greek]	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑΤRENDnet ΔΗΛΩΝΕΙ ΟΤΙ ΤΕW-721BRM ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕΚ, 2006/95/ΕΚ, 2009/125/ΕΚ και.
<b>[fr]</b> Français [French]	Par la présente TRENDnet déclare que l'appareil TEW-721BRM est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE, 2006/95/CE, 2009/125/CE et.
<b>[it]</b> Italiano [Italian]	Con la presente TRENDnet dichiara che questo TEW-721BRM è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE, 2006/95/CE e 2009/125/CE.
Latviski [Latvian]	Ar šo TRENDnet deklarē, ka TEW-721BRM atbilst Direktīvas 1999/5/ EK, 2006/95/EK, un 2009/125/EK būtiskajām prasībām un citiemar to saistītajiem noteikumiem.
Lietuvių	Šiuo TRENDnet deklaruoja, kad šis TEW-721BRM atitinka esminius reikalavimus ir kitas 1999/5/EB, 2006/95/EB ir 2009/125/EB

<b>[lt]</b> Lithuanian	Direktyvos nuostatas.
<b>[nl]</b> Nederlands [Dutch]	Hierbij verklaart TRENDnet dat het toestel TEW-721BRM in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG, 2006/95/EG, en 2009/125/EG.
<b>[mt]</b> Malti [Maltese]	Hawnhekk, TRENDnet, jiddikjara li dan TEW-721BRM jikkonforma mal-htigijiet essenzjali u ma provvedimenti oħrajn rilevanti li hemm fid-Dirrettiva 1999/5/KE, 2006/95/KE, u 2009/125/KE.
<b>[hu]</b> Magyar [Hungarian]	Alulírott, TRENDnet nyilatkozom, hogy a TEW-721BRM megfelel a vonatkozó alapvető követelményeknek és az 1999/5/EK irányelv, a 2006/95/EK és a 2009/125/EK irányelv egyéb előírásainak.
<b>[pl]</b> Polski [Polish]	Niniejszym TRENDnet oświadcza, że TEW-721BRM jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/WE, 2006/95/WE i 2009/125/WE.
<b>[pt]</b> Português [Portuguese]	TRENDnet declara que este TEW-721BRM está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE, 2006/95/CE e 2009/125/CE.
<b>[sl]</b> Slovensko [Slovenian]	TRENDnet izjavlja, da je ta TEW-721BRM v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 1999/5/ES, 2006/95/ES in 2009/125/ES.
Slovensky [Slovak]	TRENDnet tvrdí, že TEW-721BRM spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/ES, 2006/95/ES, a 2009/125/ES.
<b>[fi]</b> Suomi [Finnish]	TRENDnet vakuuttaa täten että TEW-721BRM tyyppinen laite on direktiivin 1999/5/EY, 2006/95/EY ja 2009/125/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
<b>[sv]</b> Svenska [Swedish]	Härmed intygar TRENDnet att denna TEW-721BRM står i överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG, 2006/95/EG och 2009/125/EG.

## Limited Warranty

TRENDnet warrants its products against defects in material and workmanship, under normal use and service, for the following lengths of time from the date of purchase.

TEW-721BRM – 3 Years Warranty

AC/DC Power Adapter, Cooling Fan, and Power Supply carry 1 year warranty.

If a product does not operate as warranted during the applicable warranty period, TRENDnet shall reserve the right, at its expense, to repair or replace the defective product or part and deliver an equivalent product or part to the customer. The repair/replacement unit's warranty continues from the original date of purchase. All products that are replaced become the property of TRENDnet. Replacement products may be new or reconditioned. TRENDnet does not issue refunds or credit. Please contact the point-of-purchase for their return policies.

TRENDnet shall not be responsible for any software, firmware, information, or memory data of customer contained in, stored on, or integrated with any products returned to TRENDnet pursuant to any warranty.

There are no user serviceable parts inside the product. Do not remove or attempt to service the product by any unauthorized service center. This warranty is voided if (i) the product has been modified or repaired by any unauthorized service center, (ii) the product was subject to accident, abuse, or improper use (iii) the product was subject to conditions more severe than those specified in the manual.

Warranty service may be obtained by contacting TRENDnet within the applicable warranty period and providing a copy of the dated proof of the purchase. Upon proper submission of required documentation a Return Material Authorization (RMA) number will be issued. An RMA number is required in order to initiate warranty service support for all TRENDnet products. Products that are sent to TRENDnet for RMA service must have the RMA number marked on the outside of return packages and sent to TRENDnet prepaid, insured and packaged appropriately for safe shipment. Customers shipping from outside of the USA and Canada are responsible for return shipping fees. Customers shipping from outside of the USA are responsible for custom charges, including but not limited to, duty, tax, and other fees.

**WARRANTIES EXCLUSIVE:** IF THE TRENDNET PRODUCT DOES NOT OPERATE AS WARRANTED ABOVE, THE CUSTOMER'S SOLE REMEDY SHALL BE, AT TRENDNET'S OPTION, REPAIR OR REPLACE. THE FOREGOING WARRANTIES AND REMEDIES ARE EXCLUSIVE AND ARE IN LIEU OF ALL OTHER WARRANTIES, EXPRESSED OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, STATUTORY OR OTHERWISE, INCLUDING WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

TRENDNET NEITHER ASSUMES NOR AUTHORIZES ANY OTHER PERSON TO ASSUME FOR IT ANY OTHER LIABILITY IN CONNECTION WITH THE SALE, INSTALLATION MAINTENANCE OR USE OF TRENDNET'S PRODUCTS.

TRENDNET SHALL NOT BE LIABLE UNDER THIS WARRANTY IF ITS TESTING AND EXAMINATION DISCLOSE THAT THE ALLEGED DEFECT IN THE PRODUCT DOES NOT EXIST OR WAS CAUSED BY CUSTOMER'S OR ANY THIRD PERSON'S MISUSE, NEGLIGENCE, IMPROPER INSTALLATION OR TESTING, UNAUTHORIZED ATTEMPTS TO REPAIR OR MODIFY, OR ANY OTHER CAUSE BEYOND THE RANGE OF THE INTENDED USE, OR BY ACCIDENT, FIRE, LIGHTNING, OR OTHER HAZARD.

**LIMITATION OF LIABILITY:** TO THE FULL EXTENT ALLOWED BY LAW TRENDNET ALSO EXCLUDES FOR ITSELF AND ITS SUPPLIERS ANY LIABILITY, WHETHER BASED IN CONTRACT OR TORT (INCLUDING NEGLIGENCE), FOR INCIDENTAL, CONSEQUENTIAL, INDIRECT, SPECIAL, OR PUNITIVE DAMAGES OF ANY KIND, OR FOR LOSS OF REVENUE OR PROFITS, LOSS OF BUSINESS, LOSS OF INFORMATION OR DATA, OR OTHER FINANCIAL LOSS ARISING OUT OF OR IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE, USE, PERFORMANCE, FAILURE, OR INTERRUPTION OF THE POSSIBILITY OF SUCH DAMAGES, AND LIMITS ITS LIABILITY TO REPAIR, REPLACEMENT, OR REFUND OF THE PURCHASE PRICE PAID, AT TRENDNET'S OPTION. THIS DISCLAIMER OF LIABILITY FOR DAMAGES WILL NOT BE AFFECTED IF ANY REMEDY PROVIDED HEREIN SHALL FAIL OF ITS ESSENTIAL PURPOSE.

**Governing Law:** This Limited Warranty shall be governed by the laws of the state of California.

Some TRENDnet products include software code written by third party developers. These codes are subject to the GNU General Public License ("GPL") or GNU Lesser General Public License ("LGPL").

Go to <http://www.trendnet.com/gpl> or <http://www.trendnet.com> Download section and look for the desired TRENDnet product to access to the GPL Code or LGPL Code. These codes are distributed WITHOUT WARRANTY and are subject to the copyrights of the developers. TRENDnet does not provide technical support for these codes. Please go to <http://www.gnu.org/licenses/gpl.txt> or <http://www.gnu.org/licenses/lgpl.txt> for specific terms of each license.

2014/09/10



## Product Warranty Registration

Please take a moment to register your product online.  
Go to TRENDnet's website at <http://www.trendnet.com/register>

TRENDnet  
20675 Manhattan Place  
Torrance, CA 90501. USA